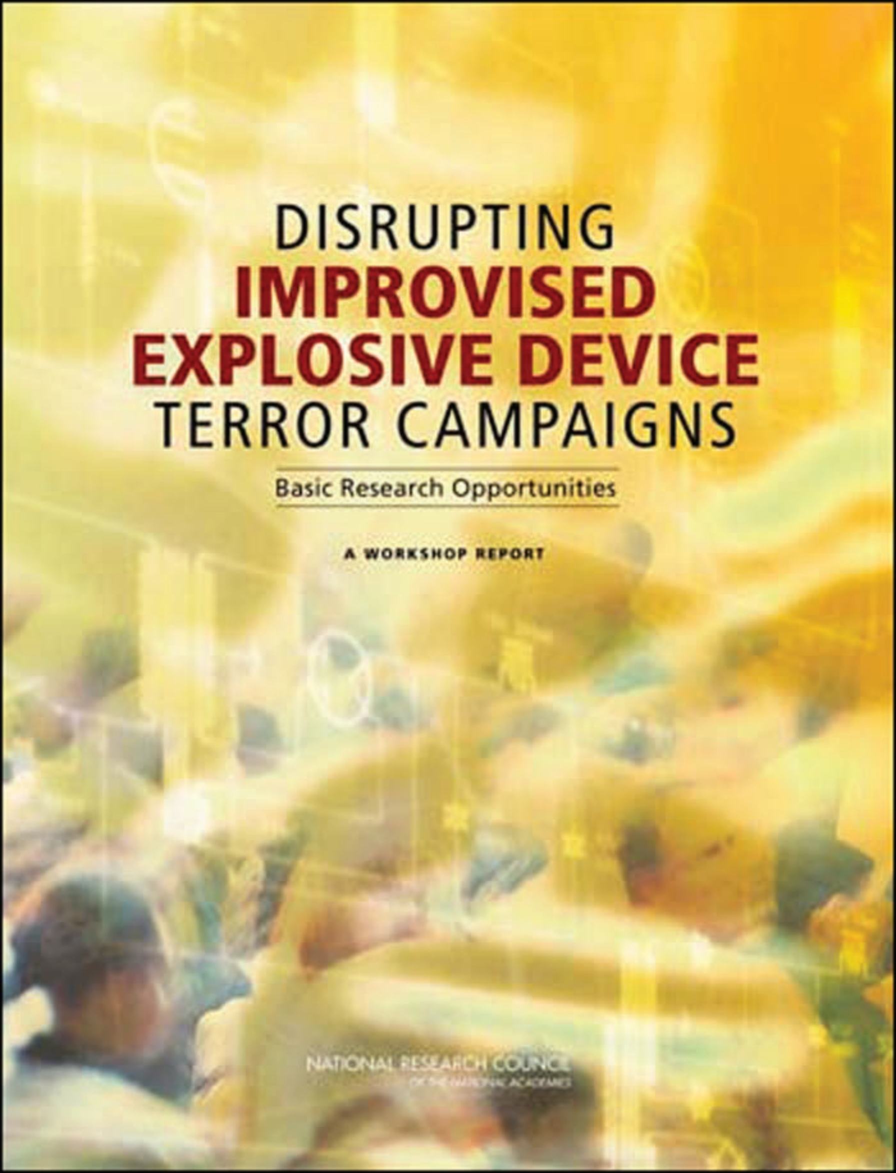

DISRUPTING IMPROVISED EXPLOSIVE DEVICE TERROR CAMPAIGNS

Basic Research Opportunities

A WORKSHOP REPORT

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Disrupting Improvised Explosive Device Terror Campaigns: Basic Research Opportunities**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The National Academies Press,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**82**	

Disrupting Improvised Explosive Device Terror Campaigns: Basic Research Opportunities

A WORKSHOP REPORT

Committee on Defeating Improvised Explosive Devices:
Basic Research to Interrupt the IED Delivery Chain

Board on Chemical Sciences and Technology
Division on Earth and Life Studies

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

THE NATIONAL ACADEMIES PRESS, 500 Fifth Street, NW Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by the Office of Naval Research, US Department of the Navy, under Grant N00014-05-G-0288.

Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-12420-1
International Standard Book Number-10: 0-309-12420-4

Additional copies of this report are available from:
The National Academies Press
500 Fifth Street, NW
Box 285
Washington, DC 20055
(800) 624-6242
(202) 334-3313 (in the Washington metropolitan area)
http://www.nap.edu

Printed in the United States of America

COMMITTEE ON DEFEATING IMPROVISED EXPLOSIVE DEVICES: BASIC RESEARCH TO INTERRUPT THE IED DELIVERY CHAIN

Chairperson

JOHN L. ANDERSON, Illinois Institute of Technology, Chicago, IL

Members

ALAN BERMAN, Independent Consultant, Alexandria, VA
CHARLES A. BOUMAN, Purdue University, West Lafayette, IN
MARTHA CRENSHAW, Stanford University, Palo Alto, CA
MARY LOU FULTZ, University of Maryland, College Park, MD
WILLIAM J. HURLEY, Institute for Defense Analyses, Alexandria, VA
ANIL K. JAIN, Michigan State University, East Lansing, MI
EDWARD H. KAPLAN, Yale University, New Haven, CT
ANDREW W. MOORE, Google, Inc., Pittsburgh, PA
JIMMIE C. OXLEY, University of Rhode Island, Kingston, RI
AMY SANDS, Monterey Institute for International Studies, Monterey, CA
WILLIAM C. TROGLER, University of California, San Diego, La Jolla, CA
JONATHAN YOUNG, Pacific Northwest National Laboratory, Richland, WA

Staff

NORMAN GROSSBLATT, Senior Editor
KATHRYN HUGHES, Associate Program Officer
KELA MASTERS, Senior Program Assistant
JESSICA L. PULLEN, Research Assistant
FEDERICO M. SAN MARTINI, Program Officer, Study Director
DOROTHY ZOLANDZ, Director, Board on Chemical Sciences and Technology

BOARD ON CHEMICAL SCIENCES AND TECHNOLOGY

PREFACE

In 2005, the Office of Naval Research (ONR) commissioned a study by the National Research Council to “examine the current state of knowledge and practice in the prevention, detection, and mitigation of the effects of improvised explosive devices (IEDs) and make recommendations for avenues of basic research.” In 2007, the National Research Council issued the report *Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities*, which identified compelling directions in basic research.

Many of the research subjects discussed in the 2007 report are worthy of much more detailed treatment than was possible in a report of such broad scope. Accordingly, the study committee that wrote the report organized and executed two workshops, which are summarized here. The workshop topics were chosen to allow ONR to explore two challenging fields of research in additional depth with a large cross-section of the research community. That served the dual purposes of helping ONR to frame its research programs and providing a forum to facilitate interactions between researchers and ONR, the Joint Improvised Explosive Device Defeat Organization, and other agencies, in particular in fields in which ONR has not traditionally been active.

The first workshop, held in February 2008 in Irvine, CA, was titled “Disrupting IED Terror Campaigns: Finding the Weak Links.” It focused on the human dimension of IED terror campaigns and on identifying basic research that could lead to improved approaches to disrupting IED terrorist organizations. Members at all levels of the organization—from leader, financier, and bomb-maker through low-level laborers—can be involved in IED activities, and understanding their roles and motivations is important in addressing the threat posed by IEDs. The workshop also considered research and perspectives on the interactions of the threat organization with the general population. The workshop brought together experts from a variety of fields, including cultural anthropology, political science, sociology, psychology, social-network analysis, game theory, communication, and criminology. Workshop participants also included people who had operational experience, including law-enforcement professionals, members of the intelligence community, and representatives of Department of Defense organizations.

The second workshop, held in March 2008 in Washington, DC, was titled “Disrupting IED Terror Campaigns: Predicting IED Activities.” Its focus was on identifying basic research that could lead to improved ability to predict IED-related activities on the basis of the collection and interpretation of data from a variety of sources—visual, electronic, material, transaction, narrative, and others. A successful and extended IED campaign usually requires the efforts of multiple people and substantial material and financial resources that generally need to be acquired from multiple sources, though single persons have succeeded in developing and deploying IEDs. It is believed that monitoring the movement of people and resources can assist in the prediction of IED-related activities and reveal an organization’s underlying structure. Therefore, development of methods for collecting and analyzing data related to those movements has been identified as a key element in countering the IED threat. Effective collection, integration, and interpretation of data are challenging—and promising—subjects of basic research aimed at mitigating the threat posed by IED terror campaigns. The workshop brought together experts from a variety of fields, including statistics, social sciences, cultural anthropology, forensic sciences, information sciences, web analytics, and mathematics.

The purpose of the workshops was to identify basic-research questions. This report summarizes the presentations and discussions that occurred at the workshops and highlights key themes of each. The views expressed in this document are those of the workshop participants and are not necessarily those of the committee.

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Dr. Scott Acton, University of Virginia
Dr. Alfred Blumstein, Carnegie Mellon University
Mr. Michael Hopmeier, Unconventional Concepts, Inc.
Dr. Gary LaFree, University of Maryland, College Park
Dr. C. Bradley Moore, University of California, Berkeley
Dr. Dennis Roberson, Illinois Institute of Technology
Dr. Jacob Shapiro, Princeton University
Dr. Neil Smelser, University of California, Berkeley
Dr. Ann Speed, Sandia National Laboratories

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the report nor did they see the final draft of the report before its release. The review of this report was overseen by Dr. R. Stephen Berry, University of Chicago. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were considered carefully. Responsibility for the final content of the report rests entirely with the authoring committee and the institution.

CONTENTS

SUMMARY

The term *improvised explosive device* (IED) has become synonymous with the current bombings in Iraq and Afghanistan, but use of the devices predates those conflicts. IEDs have been and probably will continue to be used in insurgencies and terrorist attacks throughout the world. Other recent examples of attacks involving IEDs are bombings in Bali, Delhi, Moscow, Cairo, London, Madrid, and Oklahoma City.

Countering the threat of IEDs is a challenging, multilayered problem. The IED itself is just the most publicly visible part of an underlying campaign of violence, the IED threat chain. Improving the technical ability to detect the device is a primary objective, but understanding of the goals of the adversary; its sources of materiel, personnel, and money; the sociopolitical environment in which it operates; and other factors, such as the cultural mores that it must observe or override for support, may also be critical for impeding or halting the effective use of IEDs.

Answering some basic-research questions in the physical and social sciences could enhance disruption of IED campaigns. For example, a more complete understanding of social networks and social network theory could help to reduce a population's support for an IED organization; studying the interactions between gangs and law enforcement personnel could result in improved counter-terrorist operations; understanding how money, or other forms of barter or trade, moves through communities along informal routes could help to reduce an adversary's ability to obtain funds; and research in neuroscience, cognition, and decision theory could improve human interaction with data and improve algorithms for filtering and analyzing data that result from persistent surveillance systems.

The National Research Council recently convened a committee to write a report investigating basic research opportunities for countering the threat of IEDs (National Research Council 2007). As a follow-on to that report, it organized two unclassified workshops to allow two challenging research subjects to be explored in additional depth with a broad cross-section of the research community. The first, held in Irvine, CA, on February 14-15, 2008, focused on the human dimension of IED campaigns. The second, held in Washington, DC, on March 17-18, 2008, focused on predicting IED activities. The workshops brought together experts in the physical and social sciences, the defense community, law enforcement, and other fields. Some context for the discussions is provided below and followed by a summary of the workshop themes. The views expressed in this document are those of the workshop participants and are not necessarily those of the committee.

THE IMPROVISED EXPLOSIVE DEVICE THREAT

For the purposes of this report, an IED is defined as an explosive device that is placed or fabricated in an improvised manner; incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals; and is designed to destroy, incapacitate, harass, or distract (National Research Council 2007). IEDs always contain explosive materials, detonators, and triggering mechanisms. They may be encased and include shrapnel. Explosive devices designed to disperse chemical, biologic, or radiologic material are generally not classified as IEDs and were not considered, although they often contain an explosive dispersal component. Two characteristics of IEDs that make them attractive to insurgents and terrorists are that they can be assembled relatively easily and cheaply.

The concerted use of IEDs to achieve strategic or tactical goals is referred to as an IED campaign (National Research Council 2007). The decision to engage in such a campaign is influenced by operational objectives, ideologic factors, organizational factors, and environmental and contextual factors.

Three key characteristics of an IED campaign are its asymmetry, idiosyncrasy, and dynamic nature. IED campaigns have traditionally not been used in warfare between opposing sides of roughly equal strength (that is, symmetric warfare). Rather, they often have been used by terrorists to strike soft targets and by insurgents as weapons against a stronger enemy. Idiosyncrasy in the context of an IED campaign connotes use of an unconventional approach to achieving an objective, such as hiding a bomb in the carcass of road-kill or using a washing-machine timer to set off an explosive. The dynamic nature of IED campaigns is reflected in the measure-countermeasure cycle that is played out between the adversary and counter-IED forces. One characteristic of IED campaigns that makes them so hard to defeat is that the time that the adversary needs to adapt to a countermeasure is typically shorter than the time needed by counter-IED forces to deploy and implement IED countermeasures (National Research Council 2007). Moreover, it is often more expensive for counter-IED forces to adapt than for the adversary to adapt. Counter-IED and counterinsurgency efforts are inexorably linked, and counterinsurgency concepts can be used as tools to defeat an IED campaign (National Research Council 2007).

Those who engage in an IED campaign must develop an array of capabilities to be successful. Figure S.1 depicts one model of an IED threat chain, which includes obtaining funding and bomb materials, recruiting people, constructing the IEDs, selecting targets, delivering the devices to their targets, carrying out the attacks, observing and assessing the attacks, postattack evasion, and disseminating information about the attacks for training, propaganda, recruitment, or other purposes (National Research Council 2007). Each of those components presents opportunities to disrupt an IED campaign.

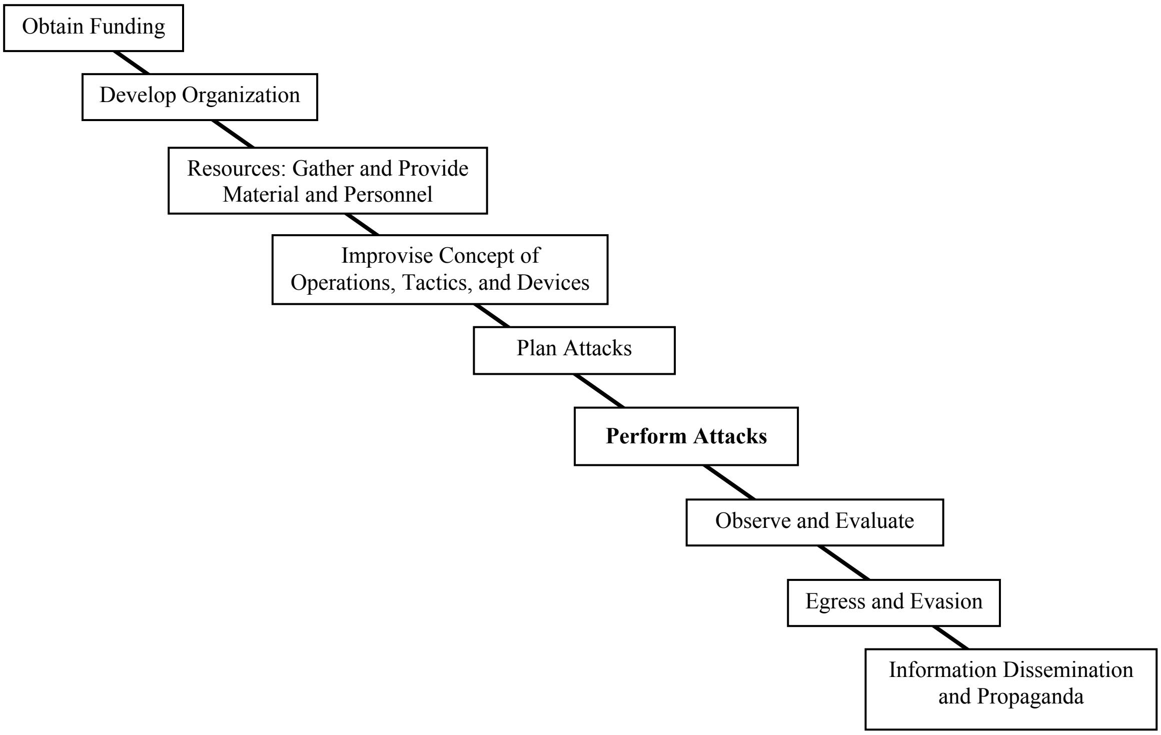
Obtain Funding
Develop Organization
Resources: Gather and Provide Material and Personnel
Improvise Concept of Operations, Tactics, and Devices
Plan Attacks
Perform Attacks
Observe and Evaluate
Egress and Evasion
Information Dissemination and Propaganda

Figure S.1 The IED threat chain (National Research Council, 2007).

WORKSHOP 1: FINDING THE WEAK LINKS

An IED campaign takes place in a local political, social, cultural, and economic environment, which has been called the human terrain. The human terrain provides the context for all counter-IED efforts. This context is a critical element in an IED campaign, but it is also the most complex and probably the least well understood (National Research Council 2007).

Five questions framed the first workshop, which focused on the human dimension of IED campaigns:

1. What are the pillars of insurgent or terrorist organizations? For example,
   - Personnel—motivation (the "cause"), leadership, recruiting, and training.
   - Resources—money, material, communication, and media access.
   - Popular support—at least to some degree (or indifference or intimidation).
   - Environment—political, economic, cultural, government, and security.
2. How do the pillars originate and evolve? How can they be affected? What opportunities and constraints do they present?
3. How do the use of IEDs in particular and terror tactics more generally depend on the pillars?
4. How can governments disrupt the processes that facilitate IED campaigns?
5. How does one measure the effect of such disruption on IED campaigns?

Five speakers gave presentations to workshop attendees to set the context for the breakout sessions that followed:

- Jeffrey M. Bale, Monterey Institute of International Studies, “Some Preliminary Observations on Jihadist Operations in Europe and IED Use”.
- Louise Richardson, Harvard University, “IEDs and the Troubles: Lessons from Northern Ireland”.
- Michael Kenney, Pennsylvania State University, “Counterterrorism Lessons from Colombia’s War on Drugs: Competitive Adaptation: Narcs vs Narcos”.
- Thomas Johnson, Naval Postgraduate School, “Lessons Learned from Afghanistan”.
- Brian Shellum, Joint Improvised Explosive Device Defeat Organization, “Insurgency in Iraq".

The breakout sessions gave participants a chance to consider basic-research questions related to disruption of personnel, resources, and community support of IED organizations.

WORKSHOP 2: PREDICTING IED ACTIVITIES

The development of capabilities that allow the prediction, prevention, or detection of the activities that precede IED emplacements would have a substantial payoff in a campaign to counter IEDs. It is believed that intelligence data—including visual, electronic, material, transactional, narrative, and other forms of data—can assist in the prediction of IED-related activities, and development of methods to enable collection and analysis of these data has been identified as a key element in countering the IED threat. Effective collection, integration, and interpretation of these data are challenging and require expansion of analytic capabilities.

Four questions framed the second workshop:

1. What data are relevant or desired to predict IED activities in an actionable manner?
2. What basic research can help to develop novel approaches and methods to manage, set priorities among, and deliver data, which may include observational and reduced data (such as analyst opinions and outputs of statistical models)?
3. What basic research is needed to allow leveraging or support of human expertise in data interpretation?
4. What basic research can lead to the development of methods that will permit more efficient analysis of large datasets that may contain diverse, incomplete, or uncertain data?

Six speakers gave presentations to workshop attendees to set the context for the breakout sessions that followed:

- Kathleen Kiernan, The Kiernan Group, “Threat Detection: Through the Eyes of Practitioners”.
- Daryl Pregibon, Google, Inc., “Overview of Toll-Fraud Detection”.
- Alexander Szalay, Johns Hopkins University, “Deploying Wireless Sensor Networks for Environmental Sensing”.

- Pramod Varshney, Syracuse University, “Data Fusion: An Enabler for Improved IED Prediction”.
- Jonathan Farley, California Institute of Technology, “Vladimir Lefebvre’s Reflexive-Control Theory and IEDs”.
- Alfred Hero, University of Michigan, “Statistical Signal Processing for IED Discovery”.

The breakout sessions gave participants a chance to consider basic-research questions related to the data that are needed and how such data could be handled, how human experience could be leveraged, and how to mixed, complex, noisy, or incomplete data can be analyzed.

WORKSHOP THEMES

Some key themes were evident in each workshop and in both.

Themes from Workshop 1

Data and Approaches Available for Analysis

Participants discussed the need for data and for approaches to analyze data. Workshop participants observed that although a large amount of data may be collected in theater, they are rarely available to researchers. Researchers need data to test models and hypotheses. The dearth of data appears to be an entrance barrier for researchers. Similarly, a lack of knowledge of the types of data that are available constrains researchers in developing new methods of analysis.

Contextual Factors Influencing a Group’s Behavioral Choices

A second theme was the importance of contextual issues and the influence of various factors on behavior. Examples include the role of religion in the decision of the Provisional Irish Republican Army not to use suicide bombings and the use of violent means other than bomb attacks. Cultural, religious, and historical factors are also critical to a community’s response to IED and counter-IED groups. For example, by understanding the cultural values of the Pashtuns, the Taliban has been able to increase the acceptability of suicide bombings within the community. Research that furthers our understanding of such issues and factors will further the development of effective counter-IED strategies. In addition, studying groups that choose *not* to use IEDs, both violent and non-violent, could be studied in order to better understand the cultural, ideological, environmental, and operational factors affecting that choice.

Public Support or Tolerance

A third theme was the vital role of public support or tolerance in an insurgency or in terrorist activities. The importance of supporting research that leads to better metrics and methods for gauging public opinion and support was stressed at the workshop. Moreover, a better understanding of the factors that shape public opinion can lead decision-makers to counter-IED measures that further the goal of “winning the hearts and minds” of the local population in a culturally appropriate manner. Advances in a broad variety of fields—such as political communication, viral marketing,[1] and marketing science—can contribute to the research.

Network and Threat Dynamics

The National Research Council’s 2007 report on IEDs noted that the adversary’s ability to learn and adapt has been an important characteristic of IED campaigns (National Research Council 2007). The dynamic nature of IED campaigns—which encompasses the network, threat, and context—was underscored throughout discussions at the workshop. It is a fundamental challenge to current counter-IED efforts. Research that leads to the development of methods and approaches for addressing dynamic problems will be particularly helpful.

A theme that was highlighted in the workshop was the learning and adaptability of not just the adversary but the counter-IED forces. The importance of recognizing that learning occurs on both sides of an IED conflict is reflected in proposed approaches, questions, and issues raised by workshop participants. For example, how can the adaptive environment be categorized? How can statistical analyses of adaptive process be developed to evaluate the effectiveness of countermeasures? How can counter-IED forces be best supported to influence, negotiate with, and collaborate with the local population? Similarly, one suggestion from a workshop participant was that corporate knowledge bases could be a useful model for developing technologies and methods to facilitate experimentation and the use of best practices among counter-IED forces.

Actions and Behaviors of the Blue Forces

A number of kinds of study can improve the effectiveness of blue[2] forces in their counterinsurgency efforts. For example, it would be helpful if the plans for an IED-based insurgency could be assessed before initiation of counterinsurgency operations. One question is whether there is a way to measure the likelihood of insurgency, and studies of civil wars might provide insight. An area’s stability could be worth monitoring, but first the factors that affect stability, their applicability among cultures, and their sensitivity to military intervention must be identified.

[1] Viral marketing uses pre-existing social networks to spread a marketing message by encouraging recipients to pass on the information.

[2] Counter-IED forces are commonly referred to as blue, civilians as green, and the adversary as red.

There are also practical concerns for blue forces. The development of technologies that could facilitate research and sharing of best practices engagement of blue forces in the human terrain could help to smooth the interactions between them and the local community. It could also improve the tactics used by blue forces in their direct counter-IED and counterinsurgency efforts.

Themes from Workshop 2

As in the first workshop, participants in the second noted the primacy of data. The broad variety of data types, the validity of data, the completeness of data, and the ubiquity of noise in data all challenge our ability to anticipate IED activities. Research that develops methods to address those challenges will be particularly helpful.

Collection, Handling, and Preprocessing of Data

Many participants felt that research in data collection, handling, and preprocessing has the potential to lead to substantial improvements in our ability to predict IED activities. The need for research that furthers data analysis, including automated filtering methods and the development of tools for analysis, was also emphasized. Research in a broad variety of fields—including electrical engineering, computer science, and statistics—can contribute to advances. One research subject of particular importance is methods for drawing inferences from data; research in statistics, risk management, and decision theory could contribute. Another theme that was evident in discussions was network modeling, especially modeling efforts that are able to capture the dynamic nature of networks in the face of partial or uncertain data.

Availability of Data for Researchers

As was the case in the first workshop, discussions throughout the second dealt with the need for publicly available databases that would allow expedient tests of models, methods, and hypotheses. Such datasets may be synthetic, be from different contexts, or be “sanitized” (so that they do not reveal specific vulnerabilities and capabilities). Making such databases available will encourage the participation of a broad variety of researchers. In particular, readily available (unclassified) databases are likely to encourage the participation of researchers who have traditionally not been involved in research sponsored by the Department of Defense (DOD) but who may bring a new perspective to research efforts.

Improvement in and Automation of Data Analysis

One of the best tools for detecting anomalies in a dataset is a human being. It is important to understand and quantify the processes used by people in making high-risk decisions on the basis of incomplete or inconsistent information. Data peculiar to the IED problem may be classified or otherwise unavailable to researchers, but other contexts can be examined fruitfully, such as the decision processes of air-traffic controllers, stock traders, and meteorologists. Research in decision theory could also focus on adversarial learning and adversarial modeling.

Research in cognitive psychology will also be useful. Some people are skilled at picking out objects or detecting changes or anomalies. Similarly, some law-enforcement personnel are able to discriminate quickly between normal and criminal behavior. Research that helps to identify behavioral attributes or metrics that enhance that ability would be useful in expanding our understanding of human information-processing capabilities and could help to improve training and data-filtration methods. In addition, research in human perception, visualization of data, and presentation of results in a user-friendly manner to aid in a decision-making is important. Such research could include neuroscience and investigate techniques for enhancing cognition. Research to enhance human-computer (mixed-initiative) decision-making will also be valuable.

Characterization of Electronic and Social Networks

IED campaigns are generally conducted by groups, and the groups form networks. Research that enhances our ability to model networks while taking into account uncertainty and the fact that the networks are dynamic could be valuable because it could further our understanding of how to influence the structure and behavior of networks. Many participants noted that the methods of modeling telecommunication activity, genetic networks, reflexive theory, and others demonstrate the variety of ways that similar problems have been addressed in different fields. A multifaceted, multidisciplinary effort in network modeling, perhaps incorporating game theory and efforts in sociology, could be useful.

Addressing the Types, Validity, and Completeness of and Noise in Datasets

The reliance of effective analysis on complete, accurate data was highlighted many times during the workshop. Data on IED activities are generally collected in adversarial, civilian environments. That can lead to incomplete datasets because of the difficulty of collecting data consistently and collecting data with large, highly variable background signals and noise. In addition, data may be acquired in any number of forms—including audio, video, handwritten notes, and measurements from wireless sensors—and may need to be fused to provide a complete picture of a situation. For such data to be used effectively in developing predictive models, they must be accurate. However, verification of data acquired in the field, such as data from human intelligence, may be difficult. Basic research in signal processing, data fusion, and system modeling could provide tools for addressing those issues.

Common Themes from Workshops 1 and 2

Need for Public Datasets

The need for public datasets to enable the participation of a broad variety of researchers was emphasized by participants in both workshops. Many academic participants expressed the belief that the lack of available data constituted a barrier to research. Although participants expressed a clear need for datasets, it was also recognized that there is a tension between research needs and national-security concerns and that constrain the Office of Naval Research and other DOD entities in making data publicly available.

DOD could take a number of creative approaches to making datasets available to researchers. Data from other conflicts, such as the Troubles in Northern Ireland and the Algerian War of Independence, or other contexts, such as counternarcotics operations and efforts to detect and counter insider trading, could provide alternative datasets for researchers to test models, methods, and hypotheses. When specific data characteristics prevent such an approach, it may be possible to create artificial (synthetic) datasets that do not reveal specific capabilities or vulnerabilities. Medical researchers and the U.S. Census Bureau have ample experience in creating databases that have been sanitized to preserve privacy, and such databases may provide a useful model. Similarly, law-enforcement agencies have made an anonymous fingerprint database available to researchers through the National Institute of Standards and Technology. That database is used by researchers to test algorithms, and competitions can be held by withholding a portion of it. DOD could use that type of model to make data available and spur interest in research in countering IEDs. Datasets to be used that way should be interactive and compatible with different needs.

Decision Theory

A second theme that was evident in both workshops was the importance of decision-making and decision theory. For example, understanding the factors that lead a group to decide to engage in violent actions and use IEDs could improve the ability to predict and prevent IED use, and understanding the factors that affect a group's decision to use particular tactics, techniques, and procedures could assist in the selection of more effective IED countermeasures. Research efforts oriented to achieving an improved understanding of the decision-making of counter-IED forces will also be valuable. For example, research to understand and quantify the processes used by people in making high-risk decisions on the basis of incomplete or inconsistent information can lead to improved decision-making in the IED context, where data are incomplete, inconsistent, or noisy. Lessons may be learned by examining the decision processes used, for example, by stock traders and in weather prediction. Similarly, better understanding of why some people are better able to than others to detect anomalies, such as the ability of former law-enforcement personnel stationed in theater to detect suspicious behavior, can lead to improved training.

Understanding Networks

Research that enhances our ability to characterize networks is another theme that was common to the two workshops. That characterization would include modeling, analysis, and the factors that influence a network. For example, how can we characterize the network of operations of an insurgent group, and what are the vulnerabilities and the dynamics of the network? Research that helps to answer such questions will enhance counter-IED capabilities. A challenge that was identified in both workshops was the difficulty of combining quantitative and qualitative data. Analytic methods that allow such data to be combined in a single framework will also be valuable.

Interdisciplinary Research

Given the broad scope of the IED problem, participants in both workshops emphasized that multidisciplinary research that integrates different disciplines should be encouraged. For example, research to develop methods for detecting telephone fraud benefited from interactions between computer scientists, statisticians, and members of the law-enforcement community. Similarly, research on insurgencies and other armed conflicts can benefit from the integration of the research of, among others, physicists, mathematicians, cultural anthropologists, operations researchers, and decision theorists. Bringing together such different research perspectives often yields the most innovative research.

1

INTRODUCTION

The term *improvised explosive device* (IED) has become synonymous with the current bombings in Iraq and Afghanistan, but use of the devices predates these conflicts by decades. IEDs have been and probably will continue to be used in insurgencies and terrorist attacks throughout the world. Other recent examples of attacks involving IEDs are bombings in Bali, Delhi, Moscow, Cairo, London, Madrid, and Oklahoma City.

Countering the threat of IEDs is a challenging, multilayered problem. The IED itself is just the most publicly visible part of the IED threat chain. Improving the technical ability to detect the device can be part of the solution, but to impede or halting the use of IEDs it may also be necessary to understand the goals of the adversary; its source of materiel, personnel, and money; the sociopolitical environment in which it operates; and other factors, such as the cultural mores that it must observe or override for support.

Answering some basic-research questions in the physical and social sciences could enhance disruption of IED campaigns. For example, a more complete understanding of social-network theory could help to reduce a population's support for an IED organization, understanding how money moves through communities along informal routes could help to reduce an adversary's ability to obtain funds, and research in neuroscience, cognition, and decision theory could improve human interaction with data and algorithms for filtering and analyzing data from persistent surveillance systems.

On February 14-15 and March 17-18, 2008, the National Research Council held two workshops to consider basic-research questions in a few of the IED-related technical and social sciences and at their interfaces. The workshops brought together experts in the physical and social sciences, defense, law enforcement, and other fields. The next sections provide some context for the discussions and the potential impact of the basic research. It should be noted that while the organizing committee is responsible for the overall quality and accuracy of the report as a record of what transpired at the workshop, the views presented here are not necessarily those of the committee.

THE IMPROVISED EXPLOSIVE DEVICE THREAT

For the purposes of this report, an IED is defined as an explosive device that is placed or fabricated in an improvised manner; incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals; and is designed to destroy, incapacitate, harass, or distract. IEDs always contain explosive materials, detonators, and triggering mechanisms (National Research Council 2007). They may be cased and include shrapnel. Explosive devices designed to disperse chemical, biologic, or radiologic material are generally not classified as IEDs and were not considered.

The concerted use of IEDs to achieve strategic or tactical goals is referred to as an IED campaign (National Research Council 2007). The decision to engage in such a campaign is influenced by operational objectives, ideologic factors, organizational factors, and environmental and contextual factors (Bale 2007).

Three key characteristics of an IED campaign are its asymmetry, its idiosyncrasy, and its dynamic nature (Meigs 2003). IED campaigns have traditionally not been used in conflicts between two opposing sides of roughly equal strength (symmetric warfare). Rather, IEDs often have been used by terrorists to strike soft targets and by insurgents as weapons against a stronger enemy. Idiosyncrasy in the context of an IED campaign connotes use of an unconventional approach to achieving an objective, such as hiding a bomb in the carcass of road-kill or using a washing-machine timer to set off an explosive. The dynamic nature of IED campaigns is reflected in the measure-countermeasure cycle that is played out between the adversary and counter-IED forces. One characteristic of IED campaigns that makes them hard to defeat is that the time that the adversary needs to adapt to a countermeasure is typically shorter than the time needed by counter-IED forces to deploy and implement countermeasures (National Research Council 2007). Counter-IED and counterinsurgency efforts are inexorably linked, and counterinsurgency concepts can be used as tools to defeat an IED campaign (National Research Council 2007).

Those who engage in an IED campaign must develop an array of capabilities to be successful. Figure 1.1 depicts an IED threat chain, which includes obtaining funding and bomb materials, recruiting people, constructing the IEDs, selecting targets, delivering the devices to their targets, carrying out the attacks, evading countermeasures after the attacks, and disseminating information about the attacks for training, propaganda, recruitment, or other purposes (National Research Council 2007). Each of those components presents opportunities to disrupt the IED campaign. For example, a campaign requires communication not only between people directly engaged in such activities as building and emplacing devices but with external sources of support and a public interface for recruitment and publicity. Similarly, a campaign needs people, materiel, money, information, facilities, and access to social networks. The operational aspects of an IED campaign—making and storing the devices, planning, attacking, and evading—also present opportunities for detection or disruption. A critical issue in countering the threat is the identification or creation of weak links in the IED threat chain.

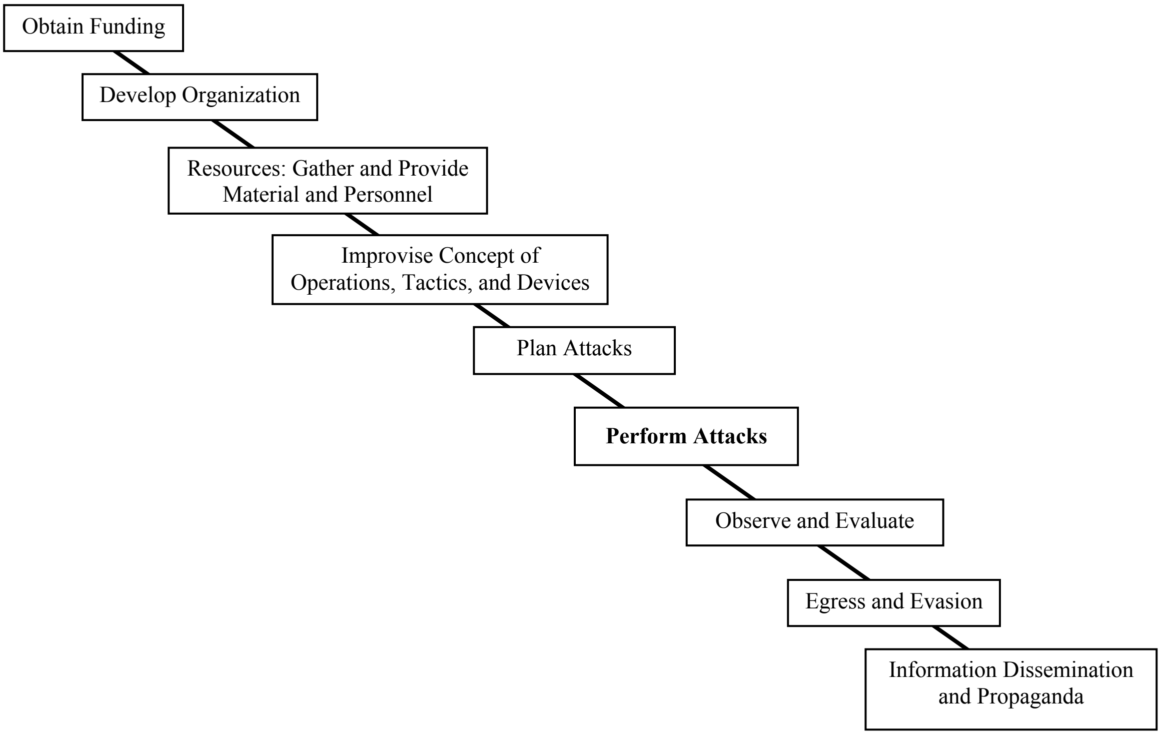
Obtain Funding
Develop Organization
Resources: Gather and Provide Material and Personnel
Improvise Concept of Operations, Tactics, and Devices
Plan Attacks
Perform Attacks
Observe and Evaluate
Egress and Evasion
Information Dissemination and Propaganda

Figure 1.1 The IED threat chain (National Research Council, 2007).

WORKSHOP 1: FINDING THE WEAK LINKS

An IED campaign does not take place in a vacuum but within the local political, social, cultural, and economic environment, which has been called the human terrain. The human terrain provides the context of all counter-IED efforts. That is a critical element in an IED campaign, but it is also the most complex and probably the least well understood (National Research Council 2007).

The first workshop focused on the human dimension of IED campaigns and asked five questions:

1. What are the pillars of insurgent or terrorist organizations? Some of the pillars are

   - Personnel—for example, motivation (the “cause”), leadership, recruiting, and training.
   - Resources—for example, money, material, communication, and mass-media access.
   - Popular support to at least some degree (or indifference or intimidation).
   - Environment—for example, political, economic, cultural, government, and security

2. How do the pillars originate and evolve? How can they be affected? What opportunities and constraints do they present?
3. How does the use of IEDs in particular, and terror tactics more generally, depend on the pillars?

4. How can governments disrupt the processes that facilitate IED campaigns?
5. How does one measure the effect of such disruption on IED campaigns?

WORKSHOP 2: PREDICTING IED ACTIVITIES

Improved prediction, prevention, or detection of the activities that precede IED emplacements may have a larger payoff then the capacity to detect an IED once it has been emplaced. That presents an opportunity, but many people and activities are generally associated with IED deployment, so prediction of IED-related activities on the basis of intelligence data—including visual, electronic, transactional, and narrative—has been identified as a key element in countering the IED threat. Effective collection, integration, and interpretation of data are crucial, and expansion of current analytic capabilities is required.

The second workshop focused asked four questions:

1. What data are relevant to or desired for the prediction of IED activities?
2. What basic research can help to develop novel approaches and methods to the management, priority-setting, and delivery of data, which may include observational and reduced data (such as analyst opinions and outputs of statistical models)?
3. What basic research is needed to allow leveraging or support of human expertise in data interpretation?
4. What basic research can lead to the development of methods that will permit more efficient analysis of large datasets that may contain diverse, incomplete, and uncertain data?

THE ROLE OF BASIC RESEARCH

Basic research is likely to have long-term payoffs. That is, basic research conducted in the near-term may not have a substantial effect in the near term on the conflicts in Iraq and Afghanistan. However, the IED threat is likely also to be a long-term phenomenon. Basic research has the potential to provide new insights and understanding to enhance our capability to counter IED campaigns at home or abroad. For example, a group's decision to engage in violent actions can be influenced by presenting disincentives (deterrence) or incentives (attractive alternatives) to members of the organization—from the leader, financier, and bomb-maker through low-level laborers—and by influencing the general population. How can one deter members? Provide attractive alternatives? It is extremely difficult (or impossible) to conduct an IED campaign successfully without public acceptance or at least tolerance. How can one influence public opinion? Those questions suggest some ways in which basic research, particularly in the social sciences, might help to counter an IED campaign. Similarly, basic research in areas such as data fusion, operations research, and statistics might also lead to improved counter-IED capabilities.

The workshops described in this report were convened with the potential benefits of basic research in mind. The summary that follows describes the presentations and discussions that took place as the participants considered basic research that would address the challenges of identifying the weak links in an organization and predicting IED activities.

2

FINDING THE WEAK LINKS (WORKSHOP 1)

The workshop on “weak links”, held in Irvine, CA, consisted of unclassified plenary and breakout sessions. The initial presentations provided participants with a context for the discussions about improvised explosive devices (IEDs) by considering past conflicts and their similarities and differences. Speakers addressed lessons and perspectives from conflicts in Iraq, Afghanistan, Northern Ireland, Colombia, and Europe. During breakout sessions, participants considered basic research questions related to disruption of personnel, resources, and community support of IED organizations.

SOME PRELIMINARY OBSERVATIONS ON JIHADIST OPERATIONS IN EUROPE AND IED USE

Jeffrey M. Bale (Monterey Institute of International Studies) spoke about four main factors that play a role in IED attacks by jihadist groups in Europe: a group’s operational objectives, ideology, and organization and the effect of environmental and contextual factors on the group.

The operational objective of IED use is usually to produce a psychologic impact at low cost. With this in mind, Bale suggested that we ask why some groups do *not* choose to use IEDs rather than focusing on why groups have embraced the use of that tactic. He attributed the reluctance to embrace IEDs to two factors: a group may be afraid of alienating its supporters by bombing, and a group may already have well-established “signature tactics” that accomplish its goals.

For jihadist groups now in Europe, ideology does not proscribe the use of IEDs. Bale cited numerous examples, from interpretations of the Qur’an to exhortations by Ayman al-Zawahiri, of jihadist ideology affirming the use of IEDs.

He stated that the most important organizational factor affecting the use of IEDs by European jihadist groups is their connection to more professional, non-European terrorist groups. It is not clear how those groups are connected to al-Qaeda or to groups in Morocco, Algeria, or Kashmir, and the relationships require further careful, empirical study. So-called home-grown groups without the connections abroad can carry out sophisticated attacks, but external support and training probably lead to more effective designs and implementation.

Bale noted that Europe “constitutes an almost ideal operating environment within which to plan and carry out IED attacks” because of the abundance of symbolic and tangible targets, such as public transportation systems and well-known monuments and symbolic locations. Western democracies also offer personal and organizational freedom that enables jihadist groups to operate with relative ease. On a practical level, radical groups take advantage of state welfare and judicial systems to spread their message and minimize the chances of effective prosecution. Finally, marginalized communities of Muslims are common on the outskirts of large cities and provide cover for jihadists wishing to "hide in plain sight".

Bale noted that his comments were preliminary. To understand the dynamics of jihadist groups using IEDs in Europe fully, it is necessary to investigate and analyze both successful and unsuccessful (failed or foiled) attacks. Carrying out in-depth case studies could enable researchers to identify trends and elucidate patterns of behavior. Similarly, the existence of marginalized communities of Muslims on the outskirts of large European cities, in addition to being a potential research topic, shows how the environment can affect operational capabilities.

During a discussion of the relative merits of qualitative and quantitative data in studying this problem, Bale indicated that his preference is for qualitative, empirical research before quantitative studies. He noted that existing databases are often incomplete and not appropriate for quantitative model-building, but acknowledged that quantitative analysis can help to identify variances in trends and qualitative research can then clarify their origins. One participant suggested that a multimethod approach might best take advantage of the strengths of each type of analysis.

IEDS AND THE TROUBLES: LESSONS FROM NORTHERN IRELAND

Louise Richardson (Harvard University) presented an overview of the conflict in Northern Ireland. She began by noting three key differences between Northern Ireland and the currently most commonly cited location of IED use, the war in Iraq: the conflict in Northern Ireland is over, it did not involve the United States, and it was resolved successfully.

IEDs of various types were used by the Provisional Irish Republican Army (IRA) during the period 1968-2005; the greatest amount of activity was in 1972-1976. IEDs were used because they were relatively inexpensive to build, could be detonated remotely, and made a strong visual impression. In addition, by attacking random targets, the IRA had a substantial effect on the psychology of the local Protestant population.

The IRA went from local use of common materials in crude explosive devices to use of more sophisticated materials in bombs in England and elsewhere. In addition to changing explosive materials, the IRA also changed its detonation method to stay ahead of the British forces: from direct detonation to remote-control switches and triggers.

The IRA also benefited from expanding its international collaborations during the Troubles.[1] It had initially focused on the local community and the resources and support available there, but later cultivated relationships with Libya, the Revolutionary Armed Forces of Colombia, Palestinian terrorist groups, and others. In the later stages, the war became more expensive in economic rather than human terms. The incidence of civilian

[1] *The Troubles* refers to the period between the late 1960s and the 1998 Belfast Agreement, and it was characterized by violence between elements of the IRA, Protestant paramilitary groups, British troops, and other parties.

bombings decreased, the IRA’s popularity waxed and waned with the bombings, and it became more effective for the group to engage in negotiations and discussions than in bombing campaigns.

Richardson identified eight major lessons learned during the Northern Ireland conflict:

- *Primacy of politics***.** About 300 members of the IRA held off 30,000 of some of the world’s best troops stationed close to home. That was recognized by the British military and government. The IRA would exist as long as the British troops were on the ground as an obvious rallying point and target.
- *Military deployment in civilian areas is difficult to manage***.** British troops were initially deployed with the understanding that they would be in Northern Ireland for only a few months, but they stayed for 38 years. The troops were initially welcomed in Catholic areas but allied themselves with the local police, who were seen as biased by the community. It took a long time for the local forces to be trained to take over policing from the military, and soldiers on the ground provided a convenient target for the IRA. Initially, it was difficult for the IRA to frame its actions as a resistance to British imperialism, because its main target was working-class Protestants. With British troops in the area, it became easier for it to justify its actions. Bloody Sunday[2] is a telling example of the difficulties that military personnel face when operating in a civilian environment. The moderate Catholic community might have accepted the actions taken by the British troops, but local support disappeared when the investigating tribunal found no fault with the actions of the British soldiers.
- *There is no substitute for good intelligence***.** It is the most important weapon in any campaign against IED organizations. British intelligence and security forces are estimated to have forestalled a great percentage of IED attacks. However, the British military initially made a grave error when it engaged in summary internment of IRA members without good intelligence. By relying on unsubstantiated, anonymous tips, it allowed the IRA to turn the technique against the soldiers by providing false tips, which led to the internment of innocents and undermined public support for the British military. Intelligence plays a key role, but any state must also fight its inherent bureaucracy.
- *Emergency legislation is never temporary.* If legislation is too one-sided or too great a deviation from standard practice, it is likely to be counterproductive. Emergency legislation may not be based on sound policy, and such measures may be difficult to remove.
- *Importance of engaging the adversary***.** The Good Friday agreement was possible only because of earlier meetings—initially disavowed by both sides—between the British government and the IRA. The agreement

[2] *Bloody Sunday* refers to Sunday, January 30, 1972, when members of the 1st Battalion of the British Parachute Regiment shot participants of a Northern Ireland Civil Rights Association march; there were 26 casualties.

allowed the negotiators to learn about the internal dynamics of the adversary. For example, the British government learned about the importance of prisoners to the IRA, and this helped to fashion the amnesty policy that was crucial to the peace agreement.

- *If a government goes too far, it learns to regret it***.** The government should not deviate too far from standard practice. For example, enactment of emergency legislation that is potentially driven by emotion rather than sound policy can have unexpected consequences.
- *Simplistic understanding of the problem increases with distance***.** The further one is from the conflict, either in time or in distance, the more simplistic the view of the problem becomes. At the site of the conflict, all the details, complexity, and facets of the problem are apparent. At a distance, it may be easier to see the "big picture" but lose sight of some of the critical issues in the field.
- *It is important to have a multipronged, integrated, military and political response to the problem***.** Any part of the government is unlikely to address all the factors that fuel an IED campaign. An integrated approach may be better to address the cultural, social, and political factors and the obvious military concerns.

Richardson stated that negotiations between a government and its adversary should initially be presented to decision-makers in pragmatic terms. Intermediaries should be used, and the meetings should be entirely deniable to allow the state to maintain credibility in the community.

On the question of why suicide bombing was not used by the IRA, she stated that suicide bombing was incompatible with the community's standards and thus was not considered an acceptable tactic. Suicide is anathema in the Roman Catholic faith, and suicide bombings would not have been accepted by the local population. However, hunger strikes they have a historical tradition in Catholicism and were used.

COUNTER-TERRORISM LESSONS FROM COLOMBIA'S WAR ON DRUGS—COMPETITIVE ADAPTATION: NARCS VS NARCOS

Michael Kenney (Pennsylvania State University) described his study of the drug trade in Colombia. This work is part of a larger comparative study of organizations that also applies competitive adaptation to the study of terrorists and counter-terrorists (Kenney 2006). He noted that there is a growing body of literature on the flexibility and adaptability of terrorist and insurgent groups. His research, however, also considers the adaptability of state security agencies.

Kenney noted that operational changes made by drug traffickers are generally tactical and are adaptations farming techniques, drug-processing, transport, distribution, and other similar systems. The adjustments are not major changes in the business model but simply improvements to exploit existing capacities. In response, enforcement personnel have adapted by moving from a focus on capturing the buyers of drugs to a focus on catching traffickers by improving intelligence collection and electronic surveillance. Various agencies have seen the value of combining efforts and skills to accomplish their goals. Drug traffickers and antidrug enforcement groups are engaged in competitive adaptation with each other, each trying to gain an advantage.

Each side's structure and goals have inherent advantages. For example, the traffickers have an information advantage in that they know where they are planning to make a delivery and do not need to know the plans of state agencies to complete their task; these organizations have less bureaucracy than state agencies and can distribute information easily. To thwart a delivery or other drug-related activity, state agencies must gather intelligence and break through the secrecy surrounding the traffickers' organizations. The state has a force advantage in that it has a much larger pool of personnel and financial support than the traffickers. When the state is successful in thwarting the traffickers' planned activities, it translates its force advantage into an information advantage by gathering intelligence and learning about the traffickers' current capabilities.

Once the state has both a force advantage and an information advantage, the traffickers must adapt to the new situation. That, in turn, forces the state to find new ways to acquire and act on intelligence. Thus, there is a constant process of competitive adaptation.

Research on similar organizations and relationships is needed to generalize that model of competitive advantage to endeavors beyond existing case studies. For example, Kenney noted that not all trafficking groups learn, and it is important to identify what leads to one group's success and another's failure. He believes that more ethnographic field work with long site visits is required and that there is too great a reliance on information acquired by journalists. Scholars also need to develop robust techniques for combining qualitative and quantitative datasets and develop formal models for these interactions.

A consideration in Kenney's model is the relative competence of the groups. Some cartels are more sophisticated than others, so general conclusions should not be drawn from the actions of a single group. The model must also consider organizational structure and leadership. For example, the compact organizational structures of some drug cartels may allow for more rapid decisions and greater adaptability than the large organizational structures that may be present in counternarcotics organizations. Similarly, if the head of an organization creates an environment in which innovation is discouraged, the adaptive learning system could be disrupted. Researchers studying similar organizations should be aware that a failure to consider a group's overall competence could introduce bias into their findings.

Kenney was asked whether Drug Enforcement Agency controls on precursor chemicals had affected drug traffickers. He thought that any initial disruption was mitigated fairly quickly because of the number of chemicals that are available and can be used in cocaine-processing.

One participant noted that achieving Kenney's goal of increasing the amount of ethnographic field research would encounter reluctance on the part of government bodies and academic researchers. On the government side, the reluctance may stem from an unwillingness to fund research on subjects considered unsafe or considered to pose a security risk. There may be a concern that the research could reveal classified information, and interactions between social researchers and the military may be difficult to negotiate. On the academic side, personal safety is certainly a concern. In addition, family obligations, language barriers, and academe's tendency not to reward this type of study may affect a researcher's decision to pursue ethnographic field research. Kenney acknowledged the issue and noted that for the field research to take place, researchers will have to be able to work with the smaller communities in which they would be studying and working. He reiterated that it is important not to rely on journalists, because they are not trained in social research and have different goals from researchers.

LESSONS LEARNED FROM AFGHANISTAN

Thomas Johnson (Naval Postgraduate School) briefed workshop participants on the current situation in Afghanistan and highlighted some of the Taliban leadership's methods for making the use of IEDs acceptable to the general population. He emphasized the need for a better general understanding of how history, culture, and community structure affect the willingness of a community to accept a given tactic and how cultural values can be exploited in counterinsurgency operations.

Since the beginning of the Iraq war, Taliban fighters have incorporated tactics from Iraq into their own insurgency. However, IEDs, and specifically suicide bombings that account for 10% of IED attacks in Afghanistan, violate the country's cultural norms. Johnson believes that, because of an inadequate understanding of the culture and of how to interact with the population, counterinsurgency forces have been unable to capitalize on that advantage. Instead, the Taliban leadership has effectively used traditional lines of communication to shift public opinion slowly in its favor.

Afghanistan has been through many occupations, and its population is well aware of the efficacy of asymmetric warfare. Suicide bombings, however, present a unique problem in that suicide is anathema to cultural norms and anonymous attacks against civilians are counter to Pashtun honor codes. The Taliban needed to work against those ingrained cultural mores to make suicide bombings acceptable. However, their familiarity with the local culture made it possible for the leaders to create new narratives about suicide bombings by using traditional community-based methods of communication, such as notices posted in public areas and word of mouth. On an individual level, the Taliban appeal to a suicide bomber's sense of religious duty and dislike of any occupying force; in some cases, the leaders appeal to a person's desire for a reward in the afterlife. On a group level, the Taliban appeal to the political objectives of a given community, highlighting a need for rebellion and the religious differences between the local population and the occupying forces and intimidating communities with the promise of retribution on their return to power.

Counterinsurgency forces are not familiar with the traditional cultural values and interactions within the Pashtun community and thus have not had notable success in countering the Taliban's message. Attacks on people in villages have offended Pashtun honor, and a lack of understanding of norms of interaction and communication has led to unwitting but important breaches in confidence and trust. For example, an image of a soldier searching a woman was used as propaganda by the Taliban, who described it as showing a violation of cultural values.

To create an effective counterinsurgency that operates within existing cultural structures, it is necessary to understand the historical and religious context of Afghan values. Traditional means of oral communication, such as a whisper campaign, could be exploited to bolster the existing aversion to IEDs. We need to study the cultural factors that influence the methods used in an insurgency. One challenge for researchers is to determine the motivations for IED use; another is to develop strategies that can help counterinsurgency forces to adapt to new environments and cultures as quickly as possible.

In response to a question, Johnson noted the need for collection of specific data. Although there is an emphasis on collecting statistics, cultural narratives and information about cultural mores are also valuable. However, it is challenging to collect, collate, verify, and distribute such information.

The Taliban appear to have had little success in causing damage in their suicide bombings. It was hypothesized that many Pashtun suicide bombers may trigger a detonation early to avoid civilian casualties (Fair 2007); that suggests that the honor code still has some effect even if the initial barrier to the action has been reduced.

Another participant noted that the situation is so complex that it is unlikely that any outsider could advance the counterinsurgency message in the Pashtun community. Johnson agreed; he recommends working with Afghans to create a whisper campaign and to operate in the community.

Finally, Johnson was asked what lessons could be taken to other conflicts. He answered that a great advantage to the Taliban was the Pashtun perception that expectations of reconstruction and greater security are unmet. That disappointment has provided a seam of discontent for the Taliban to exploit. It will be important in the future to communicate what is achievable and to keep expectations within realistic bounds.

INSURGENCY IN IRAQ

Brian Shellum (Department of Defense Joint Improvised Explosive Device Defeat Organization) updated the participants on the situation in Iraq. The recent decline in the number of successful IED attacks is attributable in part to improved counterinsurgency forces' detection capabilities and in part to changes in attitude in the population.

Shellum described five groups that have been responsible for using IEDs in Iraq and the relationships between them. By describing the general structure of the organizations, their preferred means of attack, and their supporting pillars, or motivations and goals, he demonstrated risks and tradeoffs that must be taken into account in attempting to manage relationships with these groups to turn them into allies.

Shellum noted that a number of basic factors are still poorly understood. For example, two groups may share pillars but choose different tactics; the motivations and reasoning behind the choices are not clear. How different terrorist or insurgent cells work has yet to be adequately modeled. It would be useful to characterize the differences between rural and urban cells and to map ways in which they change, grow, and regenerate.

BREAKOUT SESSION DISCUSSIONS

After the plenary session, workshop participants engaged in a series of breakout-group discussions to identify possible research opportunities. Participants were assigned to groups that mixed government representatives and academic researchers. To the extent possible, each group included a broad array of expertise. Each group was chaired by a member of the organizing committee and lasted 1 hour and 20 minutes, after which participants reconvened to discuss the groups' findings. The discussion topics were

- How to disrupt an IED organization's personnel system.
- How to disrupt an IED organization's resources.
- How to affect popular support and disrupt supportive elements of the environment.

The final session of the workshop built on the talks and breakout sessions. Participants were invited to provide feedback on overarching themes and critical research subjects highlighted during the workshop. Workshop participants represented a variety of fields of study, so different views and perspectives were expressed during the breakout discussions and plenary sessions. What follows is a general description of issues, questions, and research subjects highlighted by the reporting members of the breakout groups.

How to Disrupt an Improvised Explosive Device Organization's Personnel System

There was considerable discussion of the structure of an IED organization or cell. Some believe that an IED cell is hierarchic, with a leader, middlemen, and people who carried out specialized tasks. Others challenged that view, presenting instead a model of coalescence and fragmentation in which the structure of the IED cell is dynamic. In that model, IED cells are self-organizing systems. A cell will last long enough to carry out an attack or short series of attacks and then fragment. As counterinsurgency forces work against an IED organization, they may remove individuals or groups from a cell; some cells will collapse and others will regenerate. As Shellum had noted, basic questions about the structure and resiliency of these groups remain.

The distinctions between the hierarchic and the self-organizing cell models are important. In the former, removing key actors may make the cell ineffective; in the latter, removing a single key actor is unlikely to affect the cell's effectiveness substantially. The self-organizing model, with some additional assumptions, has been shown to produce casualty distributions that are consistent with observations of a broad variety of insurgencies and terrorist incidents (Johnson 2006, 2008). That suggests that insurgent and terrorist groups operate in the same way, regardless of the origins and locations of the conflicts. The lack of consensus on the best way to model the structure and dynamics of IED cells, and what environmental conditions generate what kind of cell, underscores the need for basic research.

Some common themes were apparent during the reporting session. The relationship between the IED organization and the local community is a key factor in determining many of the characteristics of an IED campaign. As highlighted by Johnson and Richardson, community values and attitudes affect an organization's choices. We need to understand the factors that determine the degree of community support for militants, elements of community environments that are supportive or intolerant of the use of IEDs, and the effects of a community's response to an attack. Understanding those factors will help us to know whether an organization feels it was successful in achieving its goals. The Taliban's successful use of traditional forms of communication highlights the effect that communication methods can have on public opinion and recruitment and how communication can play an important role in legitimizing or discrediting the IED organization. Would it be possible to characterize and model the role of community support and environment, the use and impact of the mass media, underlying motivations, network structure, responses to external and internal stress, and the like in these organizations?

We need research to determine patterns in organizations' motivations for choosing specific tactics. Research has not revealed why some groups choose violent tactics and others do not even when underlying motivations appear to be the same. As Bale indicated, the value of comparative studies of both historical and current organizations to answer these questions is clear. This point was emphasized by a number of the breakout groups.

Research has not clearly identified the most effective way to target IED organizations; specifically, it is unclear who the weakest and most valuable members of the organizations are, or those who are most easily influenced or subverted. For example, what motivates people to join or leave an organization? As Kenney noted, the leadership and organizational structure of different groups may impact the response of those groups to counter-IED efforts. Research that focuses on the factors that influence individual members of an IED organization, as well as differences between group and individual motivations, could inform the choice of targeting methods.

Basic research requires data, and the issue of how to acquire data, such as data on IED organizations and local communities where IEDs are used, provoked much discussion. Opportunities to collect data are always limited, so issues related to methods of collection, collation, and validation must be addressed. In some cases, it is not clear which data are the most useful for studying a given problem. Participants discussed some of the difficulties in using soldiers to collect data. Finally, as with any topic that raises questions about national security, issues of classification of data and the availability of open-source data affect how and whether many of the questions outlined above can be studied. Participants stated many times that public, relevant datasets that allow for the development and testing of models must be developed.

How to Disrupt an Improvised Explosive Device Organization's Resources

In this context of an IED organization, the definition of *resource* is important. Do resources include only physical objects and finances, or do they also include intangibles, such as tacit community support? If the definition is expanded to include the latter, a new method of capability assessment can be developed, resources categorized and sorted into classes (such as tangible and intangible), and new models of resource management and movement developed. A new theory of social resources could be investigated to study and explain how organizations take advantage of, or rely on, social factors to achieve their goals.

Chemical tagging of explosives, where possible, could be useful in identifying vulnerable parts of the supply chain. Tags could allow the tracking of movements and routes and the identification of final destinations. Tags could prove valuable in the course of forensic analysis of materials. However, as highlighted in a previous National Research Council report, questions remain about the feasibility of tagging and tracking explosive materials (National Research Council 1998). Tainting of resources could be used to undermine the confidence of members of the IED organizations and act as an indirect disruption of both resources and personnel. Participants also discussed the potential value of regulating or destroying some resources and of tracking essential materials or equipment necessary for the creation of IEDs.

IED organizations need money, barter, or trade to operate, and the merits of tracking and tagging funds, either virtually or physically, were discussed. Models of informal and traditional or community-based methods of money transfer could be developed. Separating IED-related fund transfers from legitimate commerce is challenging but important.

Finally, it is difficult to monitor and study disruptions of resources, such as materiel and money, objectively. Second-order effects of a disruption are likely, and models that could help to estimate and anticipate those effects would be beneficial. Once a disruption has been achieved, modeling and careful study may be required to obtain an accurate measure of its effectiveness in achieving the counterinsurgency's goals.

How to Affect Popular Support and Disrupt Supportive Elements of the Environment

Participants considered many angles of this broad problem. A recurring issue was teasing out which methods of affecting popular support were valid independently of the culture and which were culture-specific. For example, what elements of effective marketing techniques in the United States translate directly to other cultures and countries? Answering that question requires understanding of the role of authority and of the relative importance of personal interaction and communication in different cultures. As Johnson described in his talk, understanding and manipulating traditional methods of communication have been critical tools for the Taliban. Tracking the dissemination of messages introduced through different methods could be useful in assessing the importance to the community of different forms of communication. Better understanding of the relationships could help governments to select the best approach for affecting popular support, such as associating more closely with government or with grassroots groups.

Studying those interactions would probably require the development of robust methods to model, evaluate, and interpret data on the effect of communication on public perception. A particular challenge would be to assess the relative effects of passive and active community support and to map related trends and patterns. Such work may require a multimethod approach that uses both qualitative and quantitative data and draws from multiple fields of social-research modeling. Agent-based modeling and game theory are two examples of research areas that could contribute to such multimethod analyses. Once the models have been developed, data from past conflicts could provide rich datasets for testing and validation.

Basic questions about the social environments that sustain and support IED activities are still awaiting answers. The factors that influence the stability within communities—the dynamics of stability—are not well understood. There is a substantial literature on civil wars, but further development of models for testing and evaluating social stability in countries, regions, and villages would be valuable in assessing the likelihood of an insurgency. It would help in improving understanding of the factors that encourage or discourage groups that engage in violent activities and groups that remain nonviolent.

The work presented by Johnson and Richardson suggested that community expectations may influence its willingness to support an insurgent group. For example, the lack of electricity and other basic necessities in Iraq contravened Iraqi expectations of quick improvements after the 2003 invasion; the discrepancy between expectations and the situation on the ground probably increased support for the insurgency. Similarly, a recent publication (*The Quest for Viable Peace: International Intervention and Strategies for Conflict Transformation* 2005) argues that augmenting a government's institutional capacity drives down terrorism and insurgent activities. Investigating methods of managing expectations and of effective dissemination could be helpful in approaching unstable, potentially volatile situations. It may include investigating how different communities respond to internal and external authority. Finally, it could be useful to study the effectiveness of incentive programs in adjusting insurgent behavior or a community's support of an insurgent group.

EMERGING THEMES

Five general themes emerged from the breakout-group discussions and the final summary session of the workshop:

- Data and approaches available for analysis.
- Contextual factors that influence a group's behavioral choices.
- Public support or tolerance.
- Network and threat dynamics.
- Actions and behaviors of the "blue" forces.[3]

Some of the themes were directly related to specific counter-IED efforts, and others were related more to the social factors that influence an insurgency, whether IEDs are used or not.

Data and Approaches Available for Analysis

Research to answer any of those questions requires data. However, such data may often be difficult for researchers to access, and questions about data quality persist. The difficulty of accessing data is believed to be an "entrance barrier"—researchers could be

[3] Counter-IED forces are commonly referred to as blue, civilians as green, and the adversary as red.

encouraged to work on these subjects by making data available to test hypotheses and models. Addressing concerns about the availability of data may require creative solutions, such as creating synthetic datasets, using data from other conflicts or contexts, or "scrubbing" data to ensure that they do not reveal specific capabilities or vulnerabilities. Another option might be the development of collaborations between basic researchers and military personnel. Researchers could develop models using publicly available data that could then be tested by those with access to restricted, real-time information. The test results could be sent back to the researchers to assist in further development of the models. Methods that preserve privacy in medical research and census data may be useful models. Similarly, advances in biometrics and fingerprint analysis have been possible because test data (from which identifying information has been removed) have been made available to researchers. For example, law-enforcement agencies have been able to release fingerprints anonymously through the National Institute of Standards and Technology, and this database has been made available to researchers and used for competitions to test algorithms. The Department of Defense could use that type of model to make data available and spur interest in research on countering IEDs.

With respect to research on the ground, input from journalists may be helpful, but journalists are not social scientists and have different goals. Obtaining reliable data will require social scientists on the ground, and this in turn will require that security be sufficient for research to be conducted safely. Research that identifies methods of gathering reliable information on local cultures that harbor insurgents will be helpful. Modeling and other studies will help to determine the "right" data to obtain on an area. Conversely, in an area where there are active military operations, studies can investigate methods of obtaining relevant data by using existing sources. For example, military personnel may be too preoccupied with critical duties to fill in additional forms to contribute to basic research. It is more useful for researchers to investigate how existing data sources can be used to glean additional information. One limitation of this approach is that such data collection occurs only where military personnel are (such as in Iraq and Afghanistan). Training exercises may be useful sources of data in addition to providing insights into what data are needed and providing potential additional sources.

Contextual Factors That Influence a Group's Behavioral Choices

IEDs are relatively inexpensive and easy to manufacture and deploy and have been used effectively in different historical, cultural, and operational contexts to cause casualties. Thus, as noted by Bale, it is more useful to ask why a group that is willing to resort to violence would choose *not* to use IEDs rather than why some groups *do* use them. However, underlying both questions is the issue of why a group would resort to violence, whether the means is an IED, assassination, kidnapping, or some other act. It would be useful to know whether there are sociopsychologic discriminators that differentiate between groups that do and do not choose violence. For example, in some cases, such as the lack of suicide bombers in Northern Ireland, the decision may be strongly influenced by cultural and religious norms. Basic research can improve the understanding of the conditions under which violence becomes acceptable to groups, and what differences exist between IED organizations and others. Comparative studies may be useful in answering the question and in identifying ways to influence a group's actions. One possible source of data for such studies is the rich research literature on civil wars. Another possible subject of research is self-radicalization. Are there indicators of self-radicalization? How does it occur, especially in nonconflict zones? The studies by Silber and Bhatt (2007) and Jennifer Earl are good examples.

Public Support or Tolerance

Closely linked with the theme of contextual factors that affect behavior is the support or tolerance of the community for insurgent groups and activities. Popular support is a key element in the success or failure of an insurgency or terrorist campaign. Participants discussed many angles to the question. Is there a threshold of popular support that will make violence more likely to succeed? How can popular support be measured? Do different populations and age groups use different information outlets, such as mass media and new media? The study of the factors that influence popular support and tolerance of insurgent activities could lead to a better understanding of how to influence and undermine that support.

Network and Threat Dynamics

Past conflicts have demonstrated that dynamics and adaptation are critical aspects of an insurgency. Basic research could be helpful in characterizing the network of operations of an insurgent group and identifying the vulnerabilities and dynamics of replacement of the network. For examples, is there a minimal network size for detection or disruption purposes? Another fundamental question is how to model the structure and dynamics of IEDs cells, for example, self-organizing vs. hierarchic models of insurgent behavior. What makes some armed groups more adaptive than others? What are the interactions between insurgent groups? How important are rivalries? How important is cooperation? Statistical analyses of adaptive processes to evaluate the effectiveness of countermeasures could be useful. Studies in contexts other than armed insurgencies, such as drug smuggling and gangs, may provide useful testbeds and data. A key component of studying network adaptation is the adaptation not just of the adversary but of blue forces (for example, the counterinsurgency forces in the case of an insurgency and the "narcs" in the case of drug smuggling) and green forces (the local population).

Actions and Behaviors of the Blue Forces

A number of kinds of study can improve the effectiveness of blue forces in their counterinsurgency efforts. For example, it would be helpful if the plans for an IED-based insurgency could be assessed before initiation of counterinsurgency operations. One question is whether there is a way to measure the likelihood of insurgency, and studies of civil wars might provide insight. An area's stability could be worth monitoring, but first the factors that affect stability, their applicability among cultures, and their sensitivity to military intervention must be identified. The presence of military forces in a community probably influences it. What are the best means for military forces to negotiate and collaborate with people in the environment, including nongovernment organizations, the local population, and others? How can the viability of a host nation's government be assessed?

There are also practical concerns for blue forces. The development of technologies that could facilitate research and sharing of best practices engagement of blue forces in the human terrain could help to smooth the interactions between them and the local community. It could also improve the tactics used by blue forces in their direct counter-IED and counterinsurgency efforts.

3

PREDICTING IMPROVISED EXPLOSIVE DEVICE ACTIVITIES (WORKSHOP 2)

The second workshop focused on basic research for predicting improvised explosive device (IED) activities and consisted of unclassified plenary lectures and breakout sessions. The workshop started with presentations to provide participants with a context for the discussions about IEDs and lessons that can be learned from different disciplines and contexts. They were delivered by experts in law enforcement, computer science, statistics, mathematics, and remote sensing. The breakout sessions gave participants a chance to explore the kinds of data needed to predict IED activities and kinds of basic research that would enable the handling, priority-setting, and delivery of such data; that would allow leveraging of human expertise in data interpretation; and that might lead to procedures for analyzing mixed, complex, noisy, or incomplete data. The workshop concluded with a discussion of potential high-impact research.

THREAT DETECTION: THROUGH THE EYES OF PRACTITIONERS

Kathleen Kiernan (The Kiernan Group) spoke about some lessons from law enforcement that can be applied to a counter-IED effort. To emphasize why the law-enforcement perspective is applicable, she observed that although not every criminal is a terrorist, every terrorist is a criminal. Terrorist and criminal groups use similar methods as they recruit, learn their craft, finance operations, obtain and conceal contraband and weapons, disguise intentions, and disguise themselves with fraudulent identification.

Kiernan pointed out the lack of communication between local law enforcement and federal security agencies. A main obstacle is that most law-enforcement officers lack the level of security clearance needed to obtain and exchange information. She suggested that a database that contains low-level security information would allow the law-enforcement community to access information to help in its mission and decrease the communication divide between the two groups. She noted that it would be preferable to minimize the amount of restricted information and to control access to it.

The training and skill sets of law-enforcement officers could be helpful to military causes, and partnering could leverage the strengths of both groups. Some in the law-enforcement community have developed datasets on the methods used by gangs. Given the similarity between the methods used by gangs and those used by some terrorist and insurgent groups, such datasets could yield important lessons for the counter-IED effort. And those datasets could be made available to researchers more easily than datasets on terrorist or insurgent methods and could be valuable proxy datasets on which researchers could test theories and models of social dynamics and behavior. Examples of existing sources of such information include: the Department of Homeland Security: Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD),[4] Department of Homeland Security: Homeland Security Information Network (HSIN), [5] National Counterterrorism Center: Worldwide Incident Tracking System (WITS),[6] Department of Justice: State & Local Anti-Terrorism Training (SLATT),[7] Federal Bureau of Investigation: Law Enforcement Online (LEO),[8] International Association of Chiefs of Police (IACP),[9] Open Source Center: OpenSource.gov,[10] and the Institute for the Study of Violent Groups (ISVG),[11]

Law-enforcement professionals learn their craft on the street by dealing with human behavior. They learn to detect nuances of deception and to adapt rapidly to criminals' ever-changing tactics, behavior, and technologies. A byword on the street is "JDLR"—"just doesn't look right". The ability of law-enforcement officers' to detect anomalies, if translated to the counterinsurgency or counterterrorism context, would be helpful in detecting IED-related anomalies. Kiernan noted that many of the military personnel who are best able to detect changes and evade IEDs in Iraq are former law-enforcement officers.

Kiernan closed by saying that we need to move to the next level in the counter-IED effort. Research on networks would be helpful in identifying the crucial elements and operatives within criminal, terrorist, and insurgent groups, which is important when working against those organizations. Just as catching the easy-to-catch criminal—the small-time street dealer—is less valuable than catching those masterminding a criminal operation, catching an IED organization's bomb-maker is more useful than catching a person who is paid a small amount to emplace an IED.

OVERVIEW OF TOLL-FRAUD DETECTION

Daryl Pregibon (Google, Inc.) spoke about his experience with telephone-fraud detection. He discussed the characteristics of fraudsters (those who commit telephone-toll fraud), how to identify them, and how lessons from his experience might be useful in IED detection and prevention.

Fraudsters want free service for personal use or for resale. To commit fraud, they use a wide array of technologies to exploit weaknesses at the interfaces of technology and

[4] Department of Homeland Security: START Global Terrorism Database. http://www.start.umd.edu/data/gtd/. Accessed July 15, 2008.

[5] Homeland Security Information Network. http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm. Accessed July 15, 2008.

[6]National Counterterrorism Center: Worldwide Incident Tracking System. http://wits.nctc.gov/. Accessed July 15, 2008.

[7] Department of Justice: State & Local Anti-Terrorism Training. http://www.iir.com/slatt/. Accessed July 15, 2008.

[8]Federal Bureau of Investigation: Law Enforcement Online. http://www.fbi.gov/hq/cjisd/leo.htm. Accessed July 15, 2008.

[9] International Association of Chiefs of Police. http://www.theiacp.org/. Accessed July 15, 2008

[10] Open Source Center. www.opensource.gov. Accessed July 15, 2008.

[11] Institute for the Study of Violent Groups. http://www.isvg.org. Accessed September 16, 2008.

Fraudsters want free service for personal use or for resale. To commit fraud, they use a wide array of technologies to exploit weaknesses at the interfaces of technology and the technical barriers to information transfer. They also take advantage of the tendency for data obtained in one form by one organization to remain in that form and location. Information does not flow easily through the interfaces between business and residential telephone networks, between landlines and cellular telephones, or between voice and data networks, which makes these interfaces vulnerable to fraud. Fraudsters will adapt to prevent or delay discovery. The cycle of adaptation is similar to that in an IED campaign. Fraudsters will migrate to the telecommunication provider that is easiest to do business with, that is, the provider that is easiest to defraud. Similarly, insurgents and terrorists tend to attack the targets that are the easiest to strike, although sometimes they choose targets for their symbolic importance or for other reasons.

The problem of fraud detection in the case of telephone networks is an example of how massive datasets can be analyzed. The average large telephone-service provider covers 100 million to 1 billion active identities, of which 50-500 million are active each day. The population of telephone identities is dynamic: there might be 50,000-500,000 new and canceled users each day. That information and call data (such as the origin, destination, date, time, and length of a call) are collected and analyzed and are helpful in toll-fraud detection.

Methods of two main kinds of data analysis are used in fraud detection: anomaly detection and link-based methods. Anomaly detection uses the call history to build a signature for each caller that models how the caller acts. A customer's calls are then compared with his or her signature to scan for abnormal behaviors that may indicate a fraudster. The method works well because all calls are scanned and factored into a caller's signature. However, low-level fraud often goes undetected, as does subscription fraud (when new accounts are set up with the intent to deceive).

Link-based methods analyze calling networks to detect fraudulent behavior. A caller's "most-contacted" list (outgoing and incoming calls) is used to build a network for each person. It can be used to link a caller to other fraudsters or recently terminated accounts because, although fraudsters may change telephone numbers, they often do not change whom they call (such as friends and family). The networks can also be used to link two people on the basis of a common third party; however, this can sometimes confuse a fraudster with his or her family members because family members are often closely related within a network.

Those who engage in an IED campaign and fraudsters share many characteristics, including the following:

- They work to exploit gaps in whatever system they are infiltrating.
- They use a wide variety of technologies.
- They adapt to delay their discovery.
- They attack at the weakest point.

However, for toll fraudsters communication is an end in itself, whereas for terrorists and insurgents it is a means to an end. Moreover, fraudsters tend to be greedy and impatient. The same cannot be said for terrorists and insurgents, or at least those who are not quickly caught.

Pregibon noted that detecting IED-related activities and communication is clearly much harder than detecting toll fraud. However, although current fraud technologies would have to be adapted to be useful, they have been developed to analyze large, dynamic sets of data and have demonstrated scalability and utility. One important lesson from the toll-fraud detection problem is that data constitute a key enabler. That suggests that collecting and analyzing as many relevant data as possible and searching for patterns will allow one to maximize the chance of detecting potential IED attacks.

DEPLOYING WIRELESS SENSOR NETWORKS FOR ENVIRONMENTAL SENSING

Alex Szalay (Johns Hopkins University) discussed how lessons learned from his experience deploying wireless sensor networks for environmental sensing might be useful in countering IEDs.

The nature of scientific computing is changing. One consequence is that data are increasingly available as a result of the development of successive generations of inexpensive sensors. Large quantities of data provide an opportunity to understand a system that is being measured but also make it challenging to extract knowledge. As the need for processing larger and larger datasets increases, new methods for doing it are needed. There is no single, well-accepted public solution for dealing with large datasets (100-1,000 terabytes [1 terabyte = 10^{12} bytes]). As counter-IED surveillance datasets may also be large, the same processing challenges may apply.

Szalay suggested that in developing strategies to handle the influx of data, it is helpful to consider the main steps that are taken in producing scientific journal articles: (1) acquire data, (2) process and calibrate data, (3) transform and load data, (4) organize data to facilitate the analysis algorithm, (5) analyze data, (6) publish. A review of that breakdown suggests that one approach to accommodating large volumes of data is to bring the analysis to the data—move (3) to (5)—rather than vice versa.

If computations are executed within a database, the volume of data that needs to be transferred is minimized, and this can reduce the costs and time for download and minimize data truncation. A cluster of databases can create and send computationally inexpensive "bricks" (subsets of the datasets) to components of the cluster for analysis. That approach is being used at Johns Hopkins University (JHU) with the GrayWulf database cluster, which has a capacity of over 1 petabyte (1 petabyte = 10^{15} bytes). Szalay discussed other projects under way at JHU that must extract information from massive datasets, including the Sloan Digital Sky Survey (SDSS), which can be thought of as the genome project for the cosmos; the PAN-STARRS project, which tries to detect asteroids that may strike Earth and is currently the largest astronomy database in the world; and the Life Under Your Feet project, which uses a wireless sensor network to measure, for example, carbon dioxide emission from soil.

A unique feature of the SDSS project is the public availability of the database, SkyServer, which allows the project to tap into distributed computing power. SkyServer has seen 930,000 unique users. In contrast with the roughly 10,000 astronomers worldwide, that number indicates the level of public interest in the project. In fact, a key discovery was made by a schoolteacher who accessed the database. There are obvious security concerns in making IED-related data available to the public, but this demonstrates the potential that increasing the number of people reviewing data can hold for increasing the likelihood of anomaly identification.

For IED detection and surveillance, it is conceivable that outdoor, distributed sensor networks that send wireless signals for analysis may be used. Szalay's experience with sensors in and outside the laboratory provides valuable, practical lessons on wireless sensor networks. Before deployment, any sensor system should undergo extensive testing, including finding the limits of instrument robustness and performing field tests, to maximize the effectiveness of data collection and transmission. Factors that may be problematic include hardware failures, background noise, and natural events, such as rain. Data from wireless systems should be compared or fused with data from external sources to increase confidence in the observations.

Szalay also advised that one collect as many data in as many forms as possible, particularly in transient or singular systems, where there is only one chance to collect real-time data but the data can be analyzed as many times as necessary. Szalay prefers to organize the data first rather than perform data-processing at the collection node; this approach puts extra strain on the nodes but increases the longevity of the data library.

DATA FUSION: AN ENABLER FOR IMPROVED IED PREDICTION

Pramod Varshney (Syracuse University) spoke about the role that data fusion could play in enabling improved IED prediction.

Data fusion is the acquisition, processing, and synergistic combination of data gathered by various sources and sensors to improve the understanding of some phenomenon or to introduce or enhance intelligence and system control functions. An example of data fusion is the processing used by the human brain, which naturally fuses human sensory information to make inferences regarding the environment. Most data-fusion models are based on Bayesian networks, but other graphical models that incorporate probability theory are also used.

As an introduction to the topic, Varshney described Figure 3.1, a conceptual framework for data fusion. In this elementary model, source prescreening allocates data to various fusion stages. Level one processing, or object refinement, consists of data alignment, tracking, association, and identification. In level two, or situation refinement, inferences regarding relationships between objects, events, and a priori information are made by using contextual information and meanings. In level three, which in IED prediction can be thought of as threat refinement, inferences regarding future threats are made on the basis of computation and knowledge of the adversary. Level four, process refinement, is the monitoring and control of the fusion process and of sensor and resource allocation. Database management allows the storage of information and should accommodate rapid-retrieval requirements. The human-computer interface is where communication between a user and a computer takes place, including directives from the user or alerts from the computer.

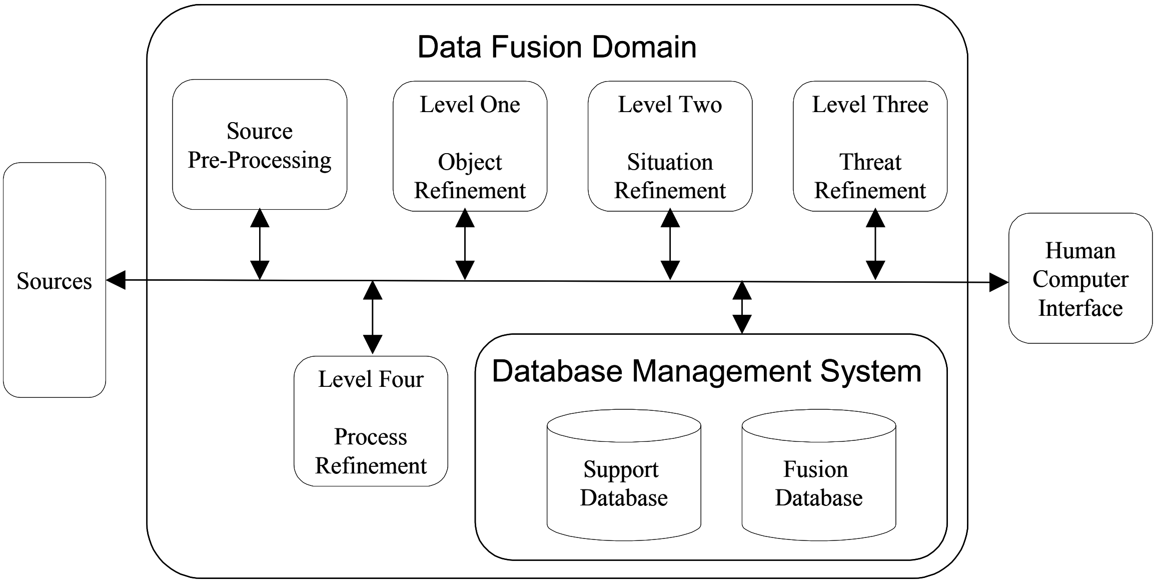

Figure 3.1 A conceptual framework for data fusion. ©1997 IEEE
NOTE: Reproduced with permission from Hall, D.L, J. Llinas, 1997. An introduction to multisensor data fusion. *Proc. IEEE* 6-23 85(1):6-23.

Research has extended that basic framework to five rather than four levels, where preprocessing is identified as the zeroth level and threat refinement is considered an impact assessment. The fifth level, added by Blasch and Plano (2003) and building on human-factors work by Endsley (1995), is user refinement. The new level allows adaptive data to be retrieved and displayed in support of decision-making.

With respect to application, the models of data fusion can be used to integrate and analyze disparate data from different sources (Xiaotao and Bir 2005; Smith and Srivastava 2004; Iyengar, Varshney, and Damarla 2007). Note that data fusion is particularly relevant to information obtained from wireless sensor networks. Such networks integrate a large number of low-cost, computationally limited processors with flexible interfaces for networking of various sensors. The network can feed the data to a fusion center. However, issues with networking and signal-processing and other system constraints must be addressed.

Data fusion is multidisciplinary in that its value is found in analyzing data from multiple sources. Developing methods that can take advantage of the variety of data types and databases available will require a large cooperative effort. Many challenges in fusing data in the IED context remain, including the treatment of social-network information and human intelligence information within databases. Current modeling of IED networks and the human terrain may not be advanced enough for appropriate training of the data-fusion models, and this may lead to spatiotemporal inference problems. In addition, the IED problem is global, dynamic, and complex, and data are being collected with many timescales, levels of accuracy, and formats. Treatment of uncertainty in particular and the handling of dependent information must be addressed.

Other technical challenges in the IED context include setting up queries to achieve an actionable result and deciding whether it is better to analyze data in or outside the database. And it must be determined whether machine learning methods can be used in a distributed setting.

One participant suggested that market-sentiment data, used in economics, could potentially yield lessons that are useful in characterizing psychologic, social, and cultural data.

VLADIMIR LEFEBVRE'S REFLEXIVE CONTROL THEORY AND IEDS

Jonathan Farley (California Institute of Technology) explained how reflexive-control theory, originally developed by Vladimir Lefebvre, could be used in a counter-IED context. In traditional mathematical approaches, a person trying to deter IED activities—the decision-maker—is passive and thus does not take into account his or her ability to preemptively influence an adversary's actions. In contrast, reflexive control presumes that the decision-maker not only predicts an adversary's actions but at least partially determines those actions by his or her own actions. A central goal is to develop methods to influence the adversary's decision-making process by manipulating the adversary's perception of reality. Thus, reflexive-control theory models the adversary's decision-making process rather than predicting the adversary's next move.

As an example, consider the following border security scenario. A decision-maker receives information that an attack will be attempted in one of three locations. Presumably, the attack will be aimed at the location where there is the perceived greatest likelihood of success. There are three possible levels of secret, nonpublic troop deployment: high, medium, and low. And there are three levels of "shows of force", public troop deployments: high, medium, and low. The problem is how to best deploy a finite number of troops to protect the anticipated attack locations and influence the adversary's decision about where to attack. That is, how should a decision-maker secretly deploy his or her forces, and what should the concurrent shows of force be? Reflexive-control theory provides a framework to solve that problem. Anticipated attack locations are modeled by assigning each location a difficulty level and a risk level. Each location is evaluated to determine the probability that it will be the next target.

As another example, suppose that in a given geographic area there are three community centers that are friendly (blue in Figure 3.2) to a decision-maker and two that are unfriendly (red). A diffusion model of public opinion provides insight into the best way to allocate public-relations resources to achieve maximal goodwill in the community. According to the diffusion model in Figure 3.2 and given that public-relations resources can be allocated to only three of the five community centers, having good relations with A, D, and E will generate the most good will in the community.

The value of such an approach is determined in part by how well the diffusion model captures the diffusion of public opinion. Improvements are needed in this area, including the development of more realistic network models and models that account for people's behaving dynamically. Diffusion models should be tested in real situations. The spread and control of public opinion may follow some of the same patterns as the spread of disease outbreaks, so a research partnership with epidemiologists could be valuable.

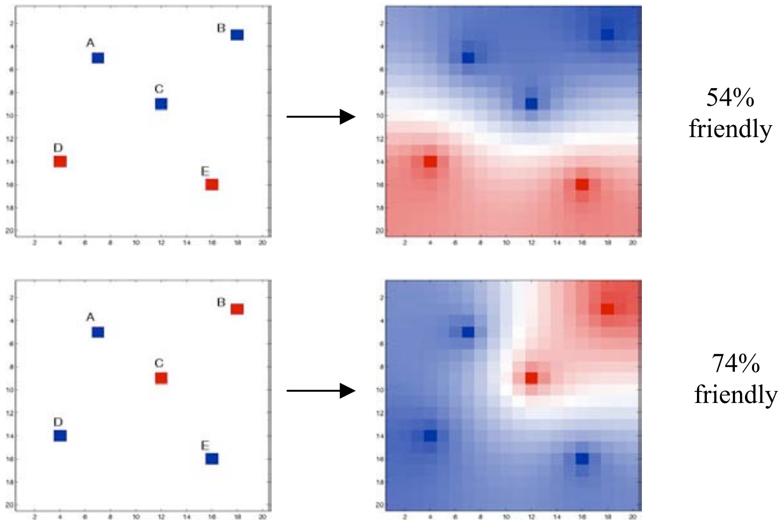

Figure 3.2 Diffusion model demonstrating how reflexive-control theory can be used to identify the best allocation of resources to achieve a specific goal (increase in blue). Courtesy of Jonathan Farley.

Farley also discussed other mathematical approaches that could be useful in the IED problem, including formal concept analysis and the theory of partially ordered sets.

STATISTICAL SIGNAL PROCESSING FOR IED DISCOVERY

Alfred Hero (University of Michigan) discussed the application of statistical signal processing to IED discovery. Many potential sources of signals are relevant to IED detection, such as video, aerial photographs, sequence of wireless personal digital assistant signals, and Internet binary signals. Such a collection of signals implies a complex, high-dimensional problem space. The signals may be mixed, including signals that are continuous and discrete and signals that are stationary and nonstationary; these variations pose special challenges for analysis. In addition, the IED problem occurs in an adversarial environment where the agents being measured may detect that they are being measured and adjust their behavior accordingly. The latter issue makes signal processing particularly challenging in the case of IEDs. However, predictive models have been developed for other complex, high-dimensional signal processing problems—for example, in telecommunication, “electronic nose” sensor arrays, Internet traffic, and genetics networks—and the results may be applicable to IED discovery.

Developing an analytic method for discovery in a complex system requires observations from the field and relevant contextual information to build a function that can be used to estimate or predict the state of the system. (Is the situation normal, or has an anomaly occurred?) The challenge is to design the function, also known as a predictor, so that it minimizes the chances of error in the result. Functions are derived from datasets, and the fundamental analytic constraints imposed by the datasets must be observed.

Any developed function or model must be iteratively “trained” and tested on appropriate datasets. During the training period, the developer identifies all the parameters necessary to model the behavior of a dataset adequately. During the test period, the developer runs the model against another, similar dataset to ensure that the model is not limited to one system. It is important to note that if the function or model has too many parameters or degrees of freedom, it may appear to accommodate any dataset but be inaccurate. If the model has too few parameters to fit the data accurately, a bias may be introduced into the analysis. Thus, any proposed model should be run against multiple surrogate datasets similar to the actual test data to check for inaccuracies.

Anomaly detection requires that statistically significant deviations from the normal baseline be reliably identifiable or "predictable". That is a challenge particularly when one is faced with a shifting, noisy baseline, and any reliable model must incorporate some form of training to accommodate such changes. One way to address that is to use a hierarchic Bayes model to test the function. A prediction is tested against a series of functions that have been increasingly conditionally constrained to test the limits and accuracy of prediction. Each successive function describes the model system more narrowly by imposing conditions on the analysis that have been derived from known contextual information. By performing this type of analysis on datasets from the same system that have been acquired at different times (and thus have different baselines), one can identify the key components for accurately modeling data across shifting baselines. For example, detecting anomalies in internet traffic data has an important parallel to IED detection. Internet traffic has a constant baseline shift: at no two times will the volume of internet traffic be exactly the same. Similarly, detecting a cell phone call that is used to detonate an IED is difficult because the traffic of cell phone calls within a network will almost certainly also have a constant baseline shift. This constantly shifting baseline requires that methods to construct a reliable predictor use online training that allows for changes in the baseline and the underlying nominal distribution.

Other approaches can be used for anomaly detection. One is based on the use of level sets: a geometric entropy minimization method, an adaptive nonparametric method based on a class of entropic graphs called *K*-point minimal spanning trees (Hero 2007), is used. Another is based on dimensional estimation with entropic graphs (Carter, Raich, and Hero 2007).

Network tomography[12] is another field of research with potential applicability to IED discovery. Rabbat and co-workers (2006; 2005) explored the problem of identifying the topology of a telephone network by using observations in the network, and Justice and Hero (2006) addressed the problem of tracking a suspect through an unknown network by using a Bayesian hierarchic prior model that accounts for changes in topology.

Similar approaches have been applied to gene-pathway reconstruction (Rabbat, Figueiredo, and Nowak 2007). The main objective is to discover signaling pathways, sequences of transcription factors for gene expression that are expressed in a time-dependent way. Because pathways are not known a priori, they are estimated by applying a stimulus and observing a response. That type of interaction has parallels to social-network settings in IED detection.

Electronic-nose sensor arrays address a similar issue that arises when the signal response from a diverse array of sensing elements is used to train the array to detect a

[12] Network tomography is the field of inferential network monitoring, in which internal characteristics of a network are inferred by using information derived from end-point data.

specific chemical. Such methods as linear discriminant analysis have been applied to this type of problem with the advantages that training can minimize errors, and validation is based on the model's predictive power for other datasets (Feldhoff, Saby, and Bernadet 1999). Other methods used to analyze an array of inputs include principal-component analysis (Pardo et al. 2006). More advanced methods of pattern recognition—including probabilistic and artificial neural networks, nearest-neighbor classification, binary recursive classification, maximal-margin classification, bootstrap aggregation, and machine-learning decision-tree sampling (for example, random forest classification)—might be applicable to classification of quantifiable data on the human terrain.

Research in signal processing has the potential to improve counter-IED capabilities. The complexity of data collected in studying the IED problem means that there observations will probably be inadequate to develop a fully predictive model, and tradeoffs will have to be made between the richness of expression of a model and overfitting of the model on incomplete data sets. Incomplete data means that preanalysis will be helpful in allocating resources to collect data. Additional challenges posed by the IED-detection problem include the need for a low-dimensional feature space to keep the problem manageable and the timeliness required because relevant information must be used quickly before the situation on the ground changes.

BREAKOUT SESSION DISCUSSION

After the plenary session, workshop participants engaged in a series of breakout-group discussions to identify possible research opportunities. Participants were assigned to groups that mixed government representatives and academic researchers. To the extent possible, each group included a broad array of expertise. Each discussion group was chaired by a member of the organizing committee and lasted 1 hour and 15 minutes, after which participants reconvened in a plenary session to discuss the groups' findings. The discussion topics were

- What data are needed/desired to predict IED activities, and what basic research avenues would enable the handling, prioritization, and delivery of such data?
- What research is needed to allow leveraging of human expertise in data interpretation?
- What research opportunities might lead to procedures to better analyze mixed, complex, noisy, incomplete data?

The final session of the workshop built on the talks and breakout sessions. Participants were invited to provide feedback on overarching themes and critical research subjects highlighted during the workshop. Workshop participants represented a variety of fields of study, so different views and perspectives were expressed during the breakout discussions and plenary sessions. What follows is a general description of issues, questions, and research subjects highlighted by the reporting members of the breakout groups.

Data to Predict Improvised Explosive Device Activities and Basic Research to Enable the Handling, Priority-Setting, and Delivery of Data

Participants noted that research questions determine what data need to be collected (such as why one group would use IEDs and another would not and how IED use varies among groups). Thus, the question of which data to collect is a question of priorities, and participants noted that categorizing and indexing data that already exist in preparation for analysis would be an important step toward identifying what data are most useful for predicting IED activities.

Participants considered the difficulties in determining whether general or specific questions would be most useful. The study of IEDs and their use is multifaceted and touches on many fields of study, and it is important to define the parameters for analysis carefully to achieve the desired research outcome. In addition, the multidisciplinary nature of the analysis means that communication between researchers and those collecting and aggregating the data is critical to avoiding confusion. For example, it was also noted that the definition of a dataset is different in different fields.

The environment where IEDs are used is constantly changing, so data-collection methods would ideally be robust, adaptable, and easily integrated into current protocols. It would be convenient if data-collection methods and tools worked well with the methods and tools that soldiers and others on the ground are already using. As noted by Kiernan, data-collection techniques used by law-enforcement organizations could be studied and compared with the types of data and collection methods available in a military setting.

Assuming that military personnel can be used as sensors to collect data, practical problems exist in data handling. In this context, soldiers would not be used to perform social research. Rather, the goal is better use of the data already collected by soldiers in their work. In some cases, the questions asked by military personnel could be tailored to achieve both the tactical goals and the social-research goals, but it is understood that a soldier's primary job is not gathering social-research data. Data are likely to be acquired in many forms (verbal, audio, video, word documents, handwritten notes, and so on), and there is no standard method for integrating heterogeneous data sources. Real-time translation capabilities for digital, print, and audio media are also lacking. Developing such tools will improve the ability to quantify and analyze information provided by soldiers in theater.

In using data to anticipate IED activities, signal-to-noise issues are important. These measurements are made in a civilian environment, and it is challenging to differentiate suspicious activity from the myriad innocuous tasks that a population performs every day. For example, persistent surveillance assets will result in large datasets, and these will contain a great deal of day-to-day background activity. Enhanced methods for modeling systems and networks would help to identify anomalous events that stand out from the noise. The nature of the environment in which the data are acquired may lead to incomplete datasets. Modeling may also help to compensate for errors resulting from those incomplete datasets, and may reduce the analysis required by identifying the most and least valuable portions of the collected data. Modeling may also help to develop proxy datasets for testing of analytic methods.

Methods for handling large, heterogeneous datasets must be developed for this type of analysis, including programs that can systematically characterize and filter data. New visualization and mapping techniques for viewing data could be developed to make interpretation and analysis of data easier.

Participants were concerned about the lack of available IED-related data for research purposes. There was a discussion of the potential of open-source databases as research tools. For example, could one study the use of everyday technology, such as cellular telephones and the Internet, and correlate it to IED events by using open, unclassified databases? Would it be possible to create an unclassified wiki type of database, similar to ones that have been used in astronomy research, that would enable citizens to assist in labeling IED events and identifying trends? Some basic research subjects are promising, such as developing improved methods of image identification or modeling of networks and informal financial systems, but application of the basic research to IED activities will require access to pertinent datasets.

Research Needed to Leverage Human Expertise in Data Interpretation

This discussion touched on one of the same issues as the first breakout session: the potential utility of automated prefiltering and preliminary analysis of data. Other research subjects of interest included new methods of data acquisition and aggregation; challenges in detecting anomalies in video streams; developing effective methods of data presentation and visualization for analysts and decision-makers; improving understanding, modeling, and training of human analytic abilities; and human-directed and automated gathering of information.

In many cases, the information required to anticipate IED activities must be acquired in a hostile environment. Modeling that environment may help to identify the most pertinent data to collect, determine the most effective means of collecting them, and help to interpret them. For example, the attitude of the local population toward a particular situation and the individual or group collecting the information will probably affect the data. Understanding motivating factors and issues that affect a population's response to specific activities would be useful in creating an environment favorable for data collection.

One key source of data is the soldiers and civilians on the ground in an area where IED activities are taking place. These "sensors" are human, so the quality of the information they provide is dictated by human abilities and the environment in which it is collected. Some people are better than others at identifying anomalous events and activities, what Kiernan referred to as the ability to notice when something "just doesn't look right" (JDLR). A system of data collection that relies on soldiers in the field may benefit from research on characteristics of exceptional observers, including studies of experience law enforcement personnel. Some initial questions could be what are the visual cues that soldiers use to find IEDs? How do police officers identify JDLR situations? Can these skills be trained? How do you take the skills of the best people at it and train others? A better understanding of why some people are skilled observers might make it possible to test personnel for relevant abilities and to place them in positions where they would be the most effective. It could also help to improve training programs to raise the skill level of ordinary observers.

A number of research challenges are pertinent to information acquisition and aggregation. Whether data have been collected by people and aggregated or collected with a remote surveillance device, such as a video camera, nearly real-time priority-setting of information and rapid processing and interpretation of the information are required if a system designed to predict IED activities is to be worth while. Information from reports provided by soldiers on patrol may need to be correlated with biometric data, cellular-telephone data, video of an event, external documents, and information from interrogation of suspects. Processing of those data in such a way as to make it possible to cross-reference and search through all the material is a distinct challenge. Workshop participants were particularly struck by the difficulties inherent in the processing of video and image data. Current methods of analyzing such data are inadequate.

Once a dataset has been acquired, it is necessary to validate it. Validation metrics for large, complex datasets are still being developed. Surrogate datasets available in the open literature may be of use for developing metrics and models prior to use in predicting IED activities. Participants once again noted the importance of making relevant datasets public for use in basic research.

Any acquired dataset, whether small and homogenous or large and heterogenous, must be must be reliably searchable. Tools for accommodating varied content types (such as video, audio, and textual) would enhance the correlation of events and data. Real-time translation and interpretation of digital and nondigital media would also be useful.

Methods of analyzing data for predicting IED activities must be able to highlight events that rise only slightly above the background noise of day-to-day living. Participants felt that development of automated prefiltering systems—perhaps informed by studies of the techniques used by human analysts—could substantially reduce the background noise and improve the chances of identifying suspicious activities. That may involve developing visualization methods to ease the job of the analysts or simply developing a comprehensive, searchable database.

Visualization itself can play many roles, from helping to identify anomalous events to simply presenting data in a form that lets analysts and decision-makers interpret information faster or focus their attention on particularly interesting portions or aspects of the data. Visualization is often a convenient way to highlight the layers of an analysis and allow investigators to "dig" into the data by looking through the overlaid levels. In addition, methods of visualization can be adapted customized to the problem at hand by, for example, tailoring color schemes to highlight relevant pieces of information; this could be useful in interpreting data when a quick response is required.

Humans are the best anomaly detectors currently available for some types of data. Understanding analysts' methods of correlating and interpreting data could assist in the development of analytic programs, in the improvement of visualization methods by identifying elements that require specific attention, and in the development of training methods for other analysts and personnel. Such studies could also identify tasks that are best accomplished by automated systems. Development of analytic systems that mimic an analyst's abilities to perceive changes and patterns would be valuable. Can intuition and the "Eureka!" moments be mapped and modeled? Participants also discussed the possibility of developing multi-initiative systems, whereby an analyst could coordinate the real-time collection activities of an automated data-collection system and tailor the searches and collection to focus on narrow or broad criteria as needed.

Many aspects of human analytic ability could be studied in greater detail. For example, humans are good at adapting to errors in data (such as an incorrect address on a document) and ignoring some errors as irrelevant to the overall analysis. However, although an analyst's intuition and analytic ability are valuable, mistakes will happen. A robust automated analytic system needs to be able to work smoothly around or correct human errors. Valuable lessons may be learned by studying the analytic processes of professionals who are required to analyze and interpret complex data quickly, such as air-traffic controllers, stock traders, and emergency personnel. Military personnel who are experts at detecting the visual cues indicative of an IED would also be a pool of people to study.

Those studies of these other fields could also lead to important information on the effect of state of mind on analysis. The effects of stress, emotions, pharmaceuticals, stimulants, fatigue, boredom, and the like on a person’s ability to process and manage data are unclear. Is there an optimal physical and emotional state for analyzing information? The effects of learning and experience on analytic ability are also important.

Finally, when considering the groups that use IEDs, participants felt it was important to model and understand the environment in which they operate so that effective predictive tools can be developed. That requires mapping and modeling community support, methods of adaptation in the face of stress, formal and informal movement of funds, the structure of cells, and the effect of interference on the network.

Research Opportunities to Analyze Mixed, Complex, Noisy, or Incomplete Data

In the third breakout session, participants were asked to consider research that might lead to procedures to analyze better mixed, complex, noisy, or incomplete data. Included in the question were the ideas of what research is needed to develop an improved capability to fuse data in a computationally reasonable way and what concepts and methods need to be developed to allow the integration of diverse forms of data.

The value of developing robust methods for combining quantitative and qualitative data in the study of IED activities was repeatedly raised during the discussion, and participants wished to develop metrics for analysis for both types of data.

The goal of data fusion in this context is to assist in the prediction, identification, and ideally, prevention of IED activities. Data fusion should produce either descriptive results (such as improved visualization) or predictive results. Ideally, it involves combining spatial and temporal information with demographic, social, and behavioral information.

Data analysis needs to allow for tracking of heterogeneous information (such as video, interviews, documents, and census data) and timescales (for example, continuous video stream vs. cumulative monthly activity reports) to identify correlations. For example, the asynchronous nature of the planning and implementation of IED attacks presents a particular challenge. Devices may be built and placed long before they are detonated. IED organizations will alter their tactics in response to counter-IED efforts.

Effective models need to accommodate both variable factors (such as changing tactics of red and blue forces and political and social changes) and invariable factors (such as location and the desire for detonation), and be adaptive to remain relevant. Data fusion may also require synthesis between datasets of different sizes, such as cellular-telephone records and suspect interviews. Developing methods for sorting various kinds of data—regardless of size, source, or type—into geospatial-temporal bins could be one important step in the fusion and analysis process. A universal format for translating heterogeneous data into a common framework for analysis would also be helpful.

With the fusing of data from multiple sources, it is important to understand the sensitivity and robustness of the fusion method in the face of errors or uncertainty in the original data. How confident can an analyst be in the data once they have been "translated" into a more useful form? It would also be helpful to develop an understanding of the relative strengths and weaknesses of different methods of uncertainty analysis for this type of data analysis. Video and other data are likely to be compressed for transfer, storage, and analysis. To what extent can data of different types be compressed before necessary information is lost? A related question is related to sampling. How many samples must be collected to have a particular level of confidence in the data, whatever the type? How can incomplete datasets be used for analysis, and how much uncertainty would such a dataset introduce?

As noted in the previous section, data that have been collected must be searchable. Current methods of data mining are inadequate for managing multiple forms of data. One specific example of this is the case of video searching. There has been some success in video identification of specific features, such as license plates and faces, but substantial challenges in event tracking and identification remain. For example, it is sometimes difficult to identify an IED blast automatically with video. In part, that may be due to the overwhelming noise and clutter in video. Methods to filter out some of the noise before analysis and to identify events and patterns in a series of images would be useful. Systems should also be able to handle errors in the data and still allow accurate searching and analysis. A study of the human ability to filter out minor errors in data without consequence might inform this research.

Another example of the need to develop data-mining methods that can handle multiple forms of data is the reports filed by patrols in theater. The reports can be filed weekly or biweekly, and this quickly leads to the creation of a very large number of files. Typically, the files are in Microsoft PowerPoint form and may include text, images, video, and audio data. Methods that can efficiently search these many different files, which may contain many forms of data, will be valuable.

One common suggestion was that preanalysis of data by automated systems might assist in data fusion and analysis. Because some parameters must be placed within an automated system, a method of identifying the "important" elements of a dataset is necessary. Participants noted that some people make high-risk decisions with little information in noisy environments every day (for example, emergency-room personnel, air-traffic controllers, and poker players). Some work has been done in decision theory to study such systems, and the research may yield some value in developing filters for human- and instrument-derived data on IED activities. Participants also felt that network research and operations research may offer a great deal in addressing these challenges.

EMERGING THEMES

The discussions at the workshop were wide-ranging, but a few research subjects were mentioned often enough to be considered themes:

- Collection, handling, and preprocessing of data.
- Availability of data for researchers.
- Improvement in and automation of data analysis.
- Characterization of electronic and social networks.
- Addressing the types, validity, and completeness of and noise in datasets.

Collection, Handling, and Preprocessing of Data

Another common theme in the workshop discussions was the collection, complexity, and methods of handling and treating the breadth of data relevant to predicting IED activities. Given the broad variety of data sources that are relevant to predicting IED activities, research on combining structured and unstructured data will be particularly valuable. For example, methods need to be developed to enable data from sensors (which may have varied temporal and spatial resolution) to be combined with intelligence and other information. Because the human dimension of IED campaigns is so important, an integrated approach could be beneficial in developing such methods, bringing together such fields as econometrics, engineering, psychology, and anthropology. In addition to research on combining data, research is needed on how to search for content in video and audio files and how to search many files that are created with common programs (such as Microsoft Word and PowerPoint).

Interpretation of IED-related data is complex and requires that researchers have a way of placing the results of data analysis in the context of the environment in which the data were collected. Participants felt that the modeling tools presented during the talks were indicative of the potential for researchers in disparate fields to contribute to the development of such models. That may result in the development of better models to assist in the filtering of data and identification of anomalies and result in the further development of formal models for interpreting social-network behavior.

Availability of Data for Researchers

The availability of data and the ability of researchers to test models and hypotheses against data were of major concern to workshop participants. Proxy data are useful, but it would be helpful to have a sanitized dataset that is representative of field data and that can be used to test what a patrol might look for with potentially available sensors. Such a dataset could be made available to the research community and used in a competition, with a portion of the dataset withheld to determine the competition winner. Additional data could be made available by bringing together multidisciplinary groups that are sent to training centers to collect data and return home fairly quickly to analyze and propose research. That approach was successfully followed during World War II to engage and make data available to operations researchers. However, it would not provide historical data and would have to be conducted in such a way as to avoid interference with training.

Improvement in and Automation of Data Analysis

One of the best tools for detecting anomalies in a dataset is a human being. It is important to understand and quantify the processes used by people in making high-risk decisions on the basis of incomplete or inconsistent information. Data peculiar to the IED problem may be classified or otherwise unavailable to researchers, but other contexts can be examined fruitfully, such as the decision processes of air-traffic controllers, stock traders, and meteorologists. Research in decision theory could also focus on adversarial learning and adversarial modeling.

Research in cognitive psychology will also be useful. Some people are skilled at picking out objects or detecting changes or anomalies. Similarly, some law-enforcement personnel are able to discriminate quickly between normal and criminal behavior. Research that helps to identify behavioral attributes or metrics that enhance that ability would be useful in expanding our understanding of human information-processing capabilities and could help to improve training and data-filtration methods. In addition, research in human perception, visualization of data, and presentation of results in a user-friendly manner to aid in a decision-making is important. Such research could include neuroscience and investigate techniques for enhancing cognition. Research to enhance human-computer (mixed-initiative) decision-making will also be valuable.

Characterization of Electronic and Social Networks

IED campaigns are generally conducted by groups, and the groups form networks. Research that enhances our ability to model networks while taking into account uncertainty and the fact that the networks are dynamic could be valuable because it could further our understanding of how to influence the structure and behavior of networks. Participants noted that the methods of modeling telecommunication activity, genetic networks, reflexive theory, and others demonstrate the variety of ways that similar problems have been addressed in different fields. A multifaceted, multidisciplinary effort in network modeling, perhaps incorporating game theory and efforts in sociology, could be useful.

Addressing the Types, Validity, and Completeness of and Noise in Datasets

The reliance of effective analysis on complete, accurate data was highlighted many times during the workshop. Data on IED activities are generally collected in adversarial, civilian environments. That can lead to incomplete datasets because of the difficulty of collecting data consistently and collecting data with large, highly variable background signals and noise. In addition, data may be acquired in any number of forms—including audio, video, handwritten notes, and measurements from wireless sensors—and may need to be fused to provide a complete picture of a situation. For such data to be used effectively in developing predictive models, they must be accurate. However, verification of data acquired in the field, such as data from human intelligence, may be difficult. Basic research in signal processing, data fusion, and system modeling could provide tools for addressing those issues.

4

WORKSHOP THEMES

Some key themes were evident in the two workshops. Themes that were present in the individual workshops will be discussed first, and then overarching themes common to the two.

WORKSHOP 1: DISRUPTING IED CAMPAIGNS: FINDING THE WEAK LINKS

Data and Approaches Available for Analysis

The first workshop focused on the human dimension of IED campaigns. One theme that was evident in workshop participants' discussions was the need for both data and approaches to analyze data. Workshop participants observed that although a large amount of data may be collected in theater, these data are rarely available to researchers. This lack of accessibility hampers the progress of basic research in this area. Researchers need data to test models and hypotheses; the dearth of data appears to be an entrance barrier for researchers. Similarly, a lack of knowledge of the types of data that are available constrains researchers in developing new methods of analysis.

Contextual Issues Influencing a Group's Behavioral Choices

A second theme that was evident in the first workshop was the importance of contextual issues and the influence of various factors on behavior. Examples include the role of religion in the decision of the Provisional Irish Republican Army not to use suicide bombings. Cultural, religious, and historical factors are also critical to a community's response to IED and counter-IED groups. For examples, by understanding the cultural values of the Pashtuns, the Taliban has been able to increase the acceptability of suicide bombings within the community. Research that furthers our understanding of these issues and factors will further the development of effective counter-IED strategies. In addition, studying groups that choose *not* to use IEDs, both violent and non-violent, should be studied in order to better understand the cultural, ideological, environmental, and operational factors affecting that choice.

Public Support or Tolerance

A third theme was the vital role of public support or tolerance in an insurgency or in terrorist activities. Given that vital role, it is important to support research that leads to better metrics and methods for gauging public opinion and support. Moreover, a better understanding of the factors that shape public opinion can guide decision-makers to counter-IED measures that further the goal of "winning the hearts and minds" of the local population in a culturally appropriate manner. Advances in a broad variety of fields—from political communication to viral marketing[13] and marketing science—can contribute to this research.

Network and Threat Dynamics

The National Research Council's 2007 report on IEDs noted that the ability of the adversary to learn and adapt has been an important characteristic of IED campaigns (National Research Council 2007). This dynamic nature of IED campaigns—which encompasses the network, threat, and context—was underscored throughout discussion at the workshop. It is a fundamental challenge to current counter-IED efforts. Research that leads to the development of methods and approaches that address dynamic problems will be particularly helpful.

Although the 2007 National Research Council report noted the ability of the adversary to learn and adapt, the workshop highlighted the learning and adaptability of not just the adversary but the counter-IED forces. The importance of recognizing that learning occurs on both sides of an IED conflict is reflected in proposed approaches, questions, and issues raised by workshop participants. For example, participants asked such questions as, how can the adaptive environment be categorized? How can statistical analyses of adaptive process be developed to evaluate the effectiveness of countermeasures? How can counter-IED forces be best supported to influence, negotiate with, and collaborate with the local population? Similarly, one participant suggested that corporate knowledge bases could be a useful model for developing technologies and methods to facilitate experimentation and best practices in counter-IED forces.

Actions and Behaviors of the Blue Forces

A number of kinds of study can improve the effectiveness of blue forces in their counterinsurgency efforts. For example, it would be helpful if the plans for an IED-based insurgency could be assessed before initiation of counterinsurgency operations. One question is whether there is a way to measure the likelihood of insurgency, and studies of civil wars might provide insight. An area's stability could be worth monitoring, but first the factors that affect stability, their applicability among cultures, and their sensitivity to military intervention must be identified.

[13] Viral marketing uses pre-existing social networks to spread a marketing message by encouraging recipients to pass on the information.

There are also practical concerns for blue forces. The development of technologies that could facilitate research and sharing of best practices engagement of blue forces in the human terrain could help to smooth the interactions between them and the local community. It could also improve the tactics used by blue forces in their direct counter-IED and counterinsurgency efforts.

WORKSHOP 2: DISRUPTING IED CAMPAIGNS: PREDICTING IED ACTIVITIES

Several themes were evident in the second workshop. The first was the primacy of data. The broad variety of data types, the validity of data, the completeness of data, and the ubiquity of noise in the data all challenge our ability to predict IED activities. Research that develops methods to address those challenges will be particularly helpful.

Data Collection and Analysis

Research in data collection, handling, and preprocessing has the potential to lead to substantial improvements in our ability to anticipate IED activities. Research that furthers data analysis, including automated filtering methods and the development of tools for analysis, is also needed. Research in a broad variety of fields—including electrical engineering, computer science, and statistics—can contribute to advances in those tasks. One research subject of particular importance is methods for drawing inferences from data. Research in statistics, risk management, and decision theory could contribute. Another theme that was evident in discussions was the importance of network modeling, especially modeling efforts that are able to capture the dynamic nature of networks in the face of partial and uncertain data.

Availability of Data

As in the first workshop, discussions in the second brought up the need for publicly available databases so that researchers can readily test models, methods, and hypotheses. Such datasets may be synthetic, from different contexts, or sanitized so that they do not reveal specific vulnerabilities and capabilities. Making such databases available will encourage the participation of a broad variety of researchers. In particular, readily available (unclassified) databases are likely to encourage the participation of researchers who have traditionally not been involved in Department of Defense–related research but may bring a new perspective to research efforts.

WORKSHOPS 1 AND 2

Need for Public Datasets

The need for a public dataset to enable the participation of a broad variety of researchers was emphasized by participants in both workshops. Many academic participants expressed the belief that the lack of available data was a barrier to research. Although participants expressed a clear need for datasets, it was also recognized that there is a tension between research needs and national-security concerns and that these concerns constrain the Office of Naval Research and other Department of Defense (DOD) entities in making data publicly available.

Participants stated that DOD could take a number of creative approaches to making datasets available to researchers. Data from other conflicts, such as the Troubles in Northern Ireland and the Algerian War of Independence, or other contexts, such as counternarcotics operations and efforts to detect and counter insider trading, could provide valuable datasets for researchers to use in testing models, methods, and hypotheses. In cases in which specific data characteristics prevent such an approach, it may be possible to create artificial (synthetic) datasets or datasets that have been "sanitized" to ensure that they do not reveal specific capabilities or vulnerabilities. Medical researchers and the U.S. Census Bureau have ample experience in creating databases that have been sanitized to preserve privacy and may provide a useful model. Similarly, through the National Institute of Standards and Technology, law-enforcement agencies have made an anonymous fingerprint database available to researchers. It is used by researchers to test algorithms, and competitions can be held by withholding a portion of it. DOD could use that type of model to make data available and spur interest in research in countering IEDs. The datasets should be interactive and compatible with different needs.

Decision Theory

A second theme that was evident in both workshops was the importance of decision-making and decision theory. For example, understanding the factors that lead a group to decide to engage in violent actions and use IEDs could improve the ability to predict and prevent IED use, and understanding the factors that affect a group's decision to use particular tactics, techniques, and procedures could assist in the selection of more effective IED countermeasures. In addition to the adversary's decision-making, research to understand the decision-making of counter-IED forces will be valuable. For example, research to understand and quantify the processes used by people in making high-risk decisions on the basis of incomplete or inconsistent information can lead to improved decision-making in the IED context, where data are incomplete, inconsistent, and noisy. Lessons may be learned by examining the decision processes used, for example, by stock traders and in weather prediction. Similarly, better understanding of why some people are better able to detect anomalies, such as the ability of former law-enforcement personnel stationed in theater to detect suspicious behavior, can lead to improved training. Research in decision science and neuroscience can also improve how data are presented and visualized and thus enhance analytic capabilities.

Understanding Networks

Research that enhances our ability to characterize networks is another theme that was common to the two workshops. Such characterization would include modeling, analysis, and the factors that influence a network. For example, how can we characterize the network of operations of an insurgent group, and what are the vulnerabilities and dynamics of replacement of the network? Research that helps to answer such questions will enhance counter-IED capabilities. A challenge that was identified in both workshops was the difficulty of combining "hard" and "soft" data. Analytic methods that allow data to be combined in a single framework will also be valuable.

Interdisciplinary Research

Given the broad scope of the IED problem, participants in both workshops emphasized that multidisciplinary research that integrates different disciplines should be encouraged. For example, research to develop methods for detecting telephone fraud benefited from interactions between computer scientists, statisticians, and members of the law-enforcement community. Similarly, although research in the nature of insurgencies and other armed conflicts started with a physics and mathematics perspective (Johnson 2006, 2008), cultural anthropologists, operations researchers, and decision theorists can contribute to it. Bringing together such different research perspectives often yields the most innovative research.

REFERENCES

Bale, Jeffrey M. 2007. Some Preliminary Observations on Jihadist Operations in Europe. In *Workshop on Determining a Research Agenda for Disrupting IED Terror Campaigns: Finding the Weak Links*. Irvine, CA.

Blasch, Erik P., and Susan Plano. 2003. Level 5: User Refinement to Aid the Fusion Process. Paper read at Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2003, at Orlando, FL.

Carter, Kevin M., Raviv Raich, and Alfred O. III Hero. 2007. Debiasing for Intrinsic Dimension Estimation. Paper read at Proc. IEEE Statistical Signal Processing Workshop (SSP).

Endsley, Mica R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors* 37 (1):32-64.

Fair, Christine. 2007. Suicide Attacks in Afghanistan. Place Published: United Nations Assistance Mission to Afghanistan. http://www.unama-afg.org/docs/_UN-Docs/UNAMA%20-%20SUICIDE%20ATTACKS%20STUDY%20-%20SEPT%209th%202007.pdf (accessed May 28, 2008).

Feldhoff, R., C. A. Saby, and P. Bernadet. 1999. Discrimination of diesel fuels with chemical sensors and mass spectrometry based electronic noses. *Analyst* 124 (8):1167-1173.

Hero, Alfred O. III. 2007. Geometric entropy minimization (GEM) for anomaly detection and localization. In *Advances in Neural Information Processing Systems 19*, edited by B. Schoelkopf, J. Platt and T. Hoffman. Cambridge, MA: MIT Press.

Iyengar, Satish G, Pramod K Varshney, and Thyagaraju Damarla. 2007. On the Detection of Footsteps Based on Acoustic and Seismic Sensing. Paper read at Proc. of 41st Annual Asilomar Conference on Signals, Systems and Computers, at Pacific Grove, CA.

Johnson, Neil F. 2006. The Mother (Nature) of All Wars? Modern Wars, Global Terrorism, and Complexity Science. *APS News*.

———. 2008. Common Complexity Underlying Insurgent Wars and Terrorism: A Contribution to the Workshop on Disrupting IED Terror Campaigns. In *Workshop on Disrupting IED Terror Campaigns: Finding the Weak Links*. Irvine, CA: The National Academies.

Justice, Derek, and Alfred O. III Hero. 2006. Estimation of Message Source and Destination from Link Intercepts. *IEEE Transactions on Information Forensics and Security* 1 (3):374-385.

Kenney, Michael. 2006. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park, PA: Pennsylvania State University Press.

Meigs, Montgomery. 2003. Unorthodox Thoughts about Asymmetric Warfare. *Parameters* 33 (2):4-18.

National Research Council. 1998. Containing the Threat from Illegal Bombings: An Integrated National Strategy for Marking, Tagging, Rendering Inert, and Licensing Explosives and Their Precursors. Washington, DC: The National Academies.

———. 2007. *Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities (Abbreviated Version)*. Washington, DC: The National Academies Press.

Pardo, M., B. C. Sisk, G. Sberveglieri, and N. S. Lewis. 2006. Comparison of Fisher's linear discriminant to multilayer perceptron networks in the classification of vapors using sensor array data. *Sensors and Actuators, B: Chemical* 115 (2):647-655.

The Quest for Viable Peace: International Intervention and Strategies for Conflict Transformation. 2005. Edited by J. Covey, M. J. Dziedzic and L. R. Hawley. Washington, DC: United States Institute of Peace Press.

Rabbat, Michael G., Mario A.T. Figueiredo, and Robert D. Nowak. 2006. Inferring Network Structure from Co-Occurrences. Paper read at Neural Information Processing Systems

———. 2007. Genomic Network Tomography. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*. Honolulu.

Rabbat, Michael G., John R. Treichler, Sally L. Wood, and Michael G. Larimore. 2005. Understanding the Topology of a Telephone Network via Internally-Sensed Network Tomography. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*. Philadelphia, PA.

Silber, Mitchell D., and Arvin Bhatt. 2007. Radicalization in the West and the Homegrown Threat, edited by New York City Police Department Intelligence Division. New York City.

Smith, Michael J., and Anuj Srivastava. 2004. A Bayesian Framework for Statistical Multi-Modal Sensor Fusion. Paper read at Proceedings of US Army Conference on Applied Statistics, at Atlanta, GA.

Xiaotao, Zou, and Bhanu Bir. 2005. Tracking Humans using Multi-modal Fusion. In *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Workshops - Volume 03*: IEEE Computer Society.

APPENDIX A

PARTICIPANT-GENERATED LISTS OF RESEARCH SUBJECTS

During the final session of each workshop, participants were invited, as a group, to create a list of research subjects that were discussed at the workshop and had resonated with them. At both workshops, participants' comments were recorded in real time by members of the National research Council staff and projected at the front of the room for all to review. At the first workshop, no further ordering or ranking of the list occurred, and the list of the research ideas is presented below in the order in which it was created. At the second workshop, after the list was created, participants were invited to vote up to five times to reflect their particular interest in topics. The list for the second workshop has been rearranged to reflect the voting, and subjects are listed in descending order of popularity.

WORKSHOP 1: FINDING THE WEAK LINKS (FEBRUARY 14-15, 2008)

- How do we gather reliable information on local cultures that harbor insurgents? And how do we translate this information into guidance for our operatives in the field?
- Ensure that research efforts are transferrable from one theater to another. (Don't focus on Iraq and Afghanistan!)
- Study the importance of the local population to insurgent and terrorist forces. Understand relationship between host population and red organization. What different types of relationships are there? How can they be leveraged to advantage?
- Main problem is not the IEDs, but the insurgency. How do IEDs fit into the goals of the insurgency? Why pick IEDs in a particular insurgency as opposed to other weapons or tactics? Carry out comparative studies.
- Metrics: regardless of aspect of problem, what are the metrics we want to use to assess outcomes and success? Metrics of public support, environment. State estimate of the environment, and measure dynamics on the basis of different courses of action we might take.
- What incentives can we offer people to dissuade them from participating in the insurgency or encourage them to desist, and what incentive-compatible actions might follow?

- How can we characterize the network of operations of an insurgent group, its vulnerabilities, and the dynamics of replacement of the network? (Dynamics and adaptation are key.)
- What makes some armed groups more adaptive than others?
- How can we characterize the adaptive environment, that is, look at adaptation of not just red, but also blue and green.
- Understanding interactions between different insurgent groups. For example, rivals may be important.
- How can we assess plans for countering IED-based insurgency before our operations begin?
- How to demotivate the terrorists by ensuring that they cannot win?
- The need for a large national database of sociocultural factors across various countries; data mining that we would need to construct the database.
- Need for a multidisciplinary approach to solve problem; need to integrate qualitative and quantitative approaches to get benefits of both.
- What are the expectations of the model? Is it better than, say, expert judgment? When do we need models, and for what? When is it smart not to use models?
- Value of comparative studies done systematically and measuring the same thing.
- Internationalize what we do—avoid cultural bias.
- Statistical analysis of adaptive process to evaluate effectiveness of countermeasures.
- Use of information outlets (such as mass media and new media) for specific subpopulations and age groups.
- What factors affect stability, and how sensitive are the factors across cultures before, during, and after operations?
- Is there a metric of insurgency likelihood?
- Can we develop technologies that facilitate experimentation and sharing of best practices for how the blue force can best engage in the human terrain? Corporate knowledge base could be a model.
- Work with the trainers, and so on (such as TRADOC and 29 Palms), on what data are needed. (Can include data format, and so on.) (Problem of scale—is it better to figure out what data are coming out of operational contexts?)
- How can outside actors influence internal political reform? Under what conditions is it most likely to occur? How best to market Western notions of freedom of speech, and so on, to other cultures? Does it make sense to try to market Western notions of democracy? How can cultural commercial marketing techniques be used?
- What lessons can be learned from other contexts to inform counterinsurgency operations? Nexus between crime and terrorism.
- What are the best means of supporting military forces to influence, negotiate with, and collaborate with people in the environment, including nongovernment organizations and host nationals?
- Developing frameworks for communicating sociocultural analysis to policy-makers and decision-makers.

- Competition for limited resources—to what extent does competition for resources drive conflict?
- How do we understand and assess the uncertainty of our data, given that we have huge amounts of incomplete data?
- The need for basic understanding of trust and deception across cultures (for example, how do you measure it?). Rule book for establishing trust in different cultures. How do you find out the rules?
- Resource interdiction—what are the key resources? Interdicting which ones is the most cost-effective? Technology frontier, gaming process, adaptation. Level of information needed to make interdict resources?
- Understand the relationship between ideology and insurgency and understand the role of ideology in stimulating and sustaining insurgencies.
- Persistent surveillance (see second workshop).
- Need for new development theory of social resources.
- Role of civilians on tomorrow's battlefield (civilians are no longer on the battlefield but *are* the battlefield).
- Study of roles of different types of interpersonal influence in different cultures (issues, power structure, and so on; flat vs hierarchic organizations).
- Understanding self-radicalization processes at home or not in conflict zones. (Again, do not focus only on Iraq and Afghanistan.) Understanding indicators (see also Silber et al. study). How to identify groups that blend into host nation?
- Sociopsychologic discriminators that differentiate between those who choose violence and those who do not.
- How do you assess the viability of the host-nation government?
- What groups are researchable as surrogates (for example, gangs and narcos)?
- Labeling groups and their leaders (which is also a function of size). Is there a minimal size of a network for detection or disruption purposes?

WORKSHOP 2: PREDICTING IED ACTIVITIES (MARCH 17-18, 2008)

1. Decision theory—understand and quantify processes used by people in making high-risk decisions on the basis of incomplete or inconsistent data (as in the Federal Aviation Administration, weather prediction, stock traders, and so on).
2. Find a meaningful way to combine "hard" (structured) and "soft" (unstructured) data (for example, images, text, and audio). Scientists + social scientists + econometricians + . . . = integrated interdisciplinary approach.
3. Create a sanitized dataset that is representative of field data and can be used to test what a patrol might look for by using potentially available sensors, and put this out to the research community as a challenge for a prize against a withheld dataset.
4. Adversarial modeling, adversarial learning, and decision theory.
5. Searching for content in video and audio data files; content extraction in a way that is searchable.
6. Network modeling with uncertainty and taking into account that the networks are dynamic. Learn how to influence the structure and behavior of networks.

7. Look at human element, (1) especially humans who are very skilled at picking out objects, and (2) characterize normal vs criminal vs terrorist—are there behavioral attributes or metrics that can be used to characterize them?
8. Visualization and presentation of results to humans in a user-friendly manner to aid in a decision; visualization for human perception in particular is important (and connected to neuroscience).
9. Search of files (such as Word, text documents, and PowerPoint) to retrieve relevant observations or conclusions that could affect a theater of operations.
10. Organize multidisciplinary groups, send them to training centers to collect data (for example, World War II operations researchers), and bring them home fairly quickly to do analysis and propose research. Interference with training and lack of historical data are difficulties.
11. Use of neuroscience techniques to enhance cognition; applied neuroscience.
12. Human-computer (mixed initiative) decision-making.
13. Develop a set of metrics to characterize the attitude space of support for an insurgency in a population, and gauge effects of counteractions.
14. Systems modeling and methods to analyze and model long-term patterns in the face of sparse observations in complex systems.
15. Create "Stop the IED-threat game"; open worldwide availability with prizes.
16. Use of wiki (collection of web pages that allows all users to contribute and modify data) methods to bring data from the field.
17. Establish institute for mathematical methods in counterterrorism.
18. Human-subjects experiments looking at multicultural and cross-cultural indicators of suspicious behavior.
19. Research in optical characterization:
    a. Machine translation—digitizing data to make them more user-friendly.
    b. Studying how the choice of measurement or analytic tool can affect tolerance of error rates.
20. Automatic speech and character recognition that is portable and easy to use.
21. Automatic analysis of optical video, but need IR dataset (related to item 10).
22. Study multiclass analysis of receiver operating characteristics.
23. Establish "guardian angel" program; provide support (such as video capability) to an off-site expert.
24. Integrate geospatial, temporal, and social-science data to create a single analytic environment.
25. Identify fundamental limits of detection.
26. How to advertise resource allocation so that adversary thinks that he or she is acting in his or her interest but is actually acting in ours (reflexive theory).
27. Gaming approach domestically to build IEDs, weapons of mass destruction—red-force approach.
28. How to identify a foreigner in a foreign country (a person who is out of place)?
29. Data handling:
    a. Priority-setting and filtering of data.
    b. Use of subsets of data.
    c. Distributed or centralized data processing.
    d. Archiving and use of data to test future theories.

30. Formal concept analysis to classify and draw inferences by using IED database.
31. Data needed: entities and links between entities.
32. Analysis of open-source data available for study.

APPENDIX B

LIST OF COMMITTEE MEMBERS

John L. Anderson (Chair), Illinois Institute of Technology

John L. Anderson (NAE) is the president of the Illinois Institute of Technology. Previously, Dr. Anderson served as provost, university vice president, and professor of chemical engineering at Case Western Reserve University. He served on the faculty of Cornell University for 5 years before joining the faculty at Carnegie Mellon University in 1976, where he served until 2004. Dr. Anderson is a member of the National Academy of Engineering (NAE) and has chaired the NAE Chemical Engineering section. He is a fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, and the American Institute of Medical and Biological Engineering. He is the author of more than 100 journal articles and book chapters. He received his bachelor's degree from the University of Delaware and his PhD in chemical engineering from the University of Illinois. His research subjects include membrane science, colloid science, fluid dynamics, and biotransport.

Alan Berman, Independent Consultant

Alan Berman is an independent consultant whose current clients include the Applied Research Laboratory of Pennsylvania State University, the Department of Energy's Jefferson Laboratory, the Joint Improvised Explosive Device Defeat Organization, the Domestic Nuclear Defense Organization, and the Customs and Boarder Patrol. Dr. Berman's expertise includes Navy research and development investments, space operations capabilities, information operations, and command, control, communications, computers, intelligence, surveillance, and reconnaissance programs. Dr. Berman served as dean of the Rosenstiel School of Marine and Atmospheric Sciences at the University of Miami, where he was responsible for the graduate programs in physical oceanography, marine biology, geology, geophysics, applied ocean science, and underwater acoustics; and as director of research at the Naval Research Laboratory, where he administered broad programs in basic and applied research.

Charles A. Bouman, Purdue University

Charles A. Bouman is professor of electrical and computer engineering and biomedical engineering at Purdue University. His research focuses on the use of statistical image models, multiscale techniques, and fast algorithms in applications that include medical and electronic imaging. Dr. Bouman received his PhD in electrical engineering from Princeton University and his MS from the University of California, Berkeley. He is a fellow of the Institute of Electrical and Electronics Engineers, the American Institute for Medical and Biological Engineering, the Society for Imaging Science and Technology, and the SPIE professional society.

Martha Crenshaw, Stanford University

Martha Crenshaw is a Senior Fellow in the Center for International Security and Cooperation at the Freeman Spogli Institute for International Studies and professor of political science by courtesy at Stanford University. She taught at Wesleyan University in Connecticut from 1974 to 2007. She chairs the American Political Science Association Task Force on Political Violence and Terrorism. She was a Guggenheim Fellow in 2005. She is also a lead investigator at the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a Center of Excellence of the Department of Homeland Security based at the University of Maryland. Her recent publications include "Terrorism and Global Security", in an edited volume, *Leashing the Dogs of War: Conflict Management in a Divided World* (United States Institute of Peace Press, 2007); and "Explaining Suicide Terrorism: A Review Essay", in *Security Studies* (Spring 2007).

Mary Lou Fultz, University of Maryland

Mary Lou Fultz is an independent consultant and former assistant director of the US Postal Service Crime Laboratory. Dr. Fultz was chief of the Forensic Science Laboratory for the Bureau of Alcohol, Tobacco and Firearms. She received her PhD in chemistry from the University of Maryland.

William J. Hurley, Institute for Defense Analyses

William J. Hurley is assistant director of the System Evaluation Division at the Institute for Defense Analyses (IDA). Before going to IDA in 1985, he was with the Center for Naval Analyses. Dr. Hurley has directed over 30 studies sponsored principally by the Office of the Secretary of Defense and the Navy. His work has emphasized force planning, analytic methods, and advanced technologies. Since 2000, he has focused on urban conflict and irregular warfare. In addition to his research responsibilities, from 1991 to 1998 Dr. Hurley was the associate director and then director of the Defense Science Study Group, a program of education and study that introduces young professors of science and engineering to national-security systems, organizations, and current issues. Dr. Hurley's academic background is in mathematical physics. He received a BS in physics from Boston College and a PhD in physics from the University of Rochester (1971) and has held research positions at Syracuse University and the University of Texas.

Anil K. Jain, Michigan State University

Anil K. Jain is a University Distinguished Professor in the Department of Computer Science and Engineering at Michigan State University. He received his BTech from the Indian Institute of Technology Kanpur and his MS and PhD from Ohio State University. His research interests include statistical-pattern recognition, computer vision, and biometric authentication. He received awards for best papers in 1987 and 1991 from the Pattern Recognition Society. He also received the 1996 *IEEE Transactions on Neural Networks* Best Paper Award. He is a fellow of the Institute of Electrical and Electronics Engineers, the Association for Computing Machinery, the American Association for the Advancement of Science, and the International Association for Pattern Recognition. He has received Fulbright, Guggenheim, and Humboldt awards. Holder of six patents in fingerprint-matching, he is the author of a number of books, including *Handbook of Face*

Recognition and *Handbook of Fingerprint Recognition*. He is a member of the National Research Council study team on Whither Biometrics?.

Edward H. Kaplan, Yale School of Management

Edward H. Kaplan (NAE, IOM) is the William N. and Marie A. Beach Professor of Management Sciences, professor of public health, and professor of engineering at Yale University. He received his bachelor's degree from McGill University and proceeded to graduate study at the Massachusetts Institute of Technology, where he completed three master's degrees—in operations research, city planning, and statistics—and a doctorate in urban studies. He has recently developed novel methods for quantitatively evaluating the tactical prevention of suicide bombings, including the operational effectiveness of suicide-bomber–detector schemes. Dr. Kaplan is a member of the Institute of Medicine and the National Academy of Engineering.

Andrew W. Moore, Google

Andrew Moore is director of one of Google's newest engineering offices, on Carnegie Mellon's campus in Pittsburgh, PA. Before joining Google, he was a professor of robotics and computer science at the School of Computer Science, Carnegie Mellon University. His main research interest is data mining: statistical algorithms for finding the potentially useful and statistically meaningful patterns in large masses of data. His research group, The Auton Lab, has devised several ways of performing large statistical operations efficiently, in several cases advancing the state of the art by several orders of magnitude. In 2003, he assisted in briefing President Bush on data-mining approaches for early warning of biologic attacks. He is on the advisory boards of several commercial and government organizations.

Jimmie C. Oxley, University of Rhode Island

Jimmie C. Oxley is professor of chemistry at the University of Rhode Island and co-director of the Forensic Science Partnership. After receiving her PhD from the University of British Columbia, Dr. Oxley joined the faculty of the New Mexico Institute of Mining and Technology, where she founded a PhD program in explosives and created the thermal-hazards research group. Dr. Oxley's laboratory specializes in the study of energetic materials. Most of the studies examine how and how fast those materials decompose; the goal is to understand their stability so that they may be handled safely. She received her BS from the University of California, San Diego (1971); her MS from California State University, Northridge; and her PhD from the University of British Columbia (1983).

Amy Sands, Monterey Institute of International Studies

Amy Sands is the provost and academic vice president of the Monterey Institute of International Studies. Before becoming provost, she held two other positions at the institute. Most recently, she served for 2.5 years as the dean of the Graduate School of International Policy Studies, which is dedicated to providing professional graduate international education to prepare students for careers in a global workplace. Earlier, she was the deputy director of the Center for Nonproliferation Studies for 7 years. Her responsibilities involved strategic oversight and daily management of the center's projects and activities. From August 1994 to June 1996, she was assistant director of the Intelligence, Verification, and Information Management Bureau at the US Arms Control and Disarmament Agency (ACDA). Before joining ACDA, she led the Proliferation Assessments Section of Z Division (Intelligence) at the Lawrence Livermore National Laboratory and was country risk manager of New England Merchants Bank. On leaving the government, Dr. Sands received ACDA's Distinguished Honor Award and the On-Site Inspection Agency's Exceptional Civilian Service Medal. She is a member of the Council on Foreign Relations and the International Institute for Strategic Studies.

William C. Trogler, University of California, San Diego

William C. Trogler is professor of chemistry and biochemistry at the University of California, San Diego. His current research focuses on inorganic chemistry applied to problems of technologic interest. Dr. Trogler's research group is exploring the use of photoluminescent conjugated silafluorene and silole polymers as sensors for detecting explosives and of chemoresponsive transistors of metal phthalocyanines as electronic chemical sensors for organic vapors and peroxides. He is also engaged in the synthesis of uniform hollow nanospheres of silica and titania for biomedical applications, such as drug and gene delivery in cancer therapy. He received his BA and MA in chemistry from Johns Hopkins University in 1974 and his PhD in chemistry from the California Institute of Technology in 1977. He is a fellow of the American Association for the Advancement of Science and a member of the Strategic Advisory Board for RedXDefense.

Jonathan Young, Pacific Northwest National Laboratory

Jonathan Young is head of the Safety and Risk Analysis Group of the Environmental Technology Division at Pacific Northwest National Laboratory. He has over 40 years of experience in systems and safety engineering, safety analysis, probabilistic safety assessment, and system-security activities in the aerospace and nuclear industries. He is principal instructor and course developer for numerous probabilistic safety-assessment courses in the United States and abroad. Mr. Young received his BA in mathematics from Lincoln University.

APPENDIX C

LIST OF WORKSHOP PARTICIPANTS

WORKSHOP 1: FINDING THE WEAK LINKS (FEBRUARY 14-15, 2008)

Speakers

Jeffrey M. Bale (Monterey Institute of International Studies)
Louise Richardson (Radcliffe Institute for Advanced Study)
Thomas H. Johnson (Naval Postgraduate School)
Michael C. Kenney (Pennsylvania State University)
Brian G. Shellum (Joint Improvised Explosive Device Defeat Organization)

Participants

John L. Anderson (Illinois Institute of Technology)
Nora Bensahel (RAND)
Nina M. Berry (Joint Improvised Explosive Device Defeat Organization)
Alfred Blumstein (Carnegie Mellon University)
Christopher Brown (Office of Naval Research)
Judee Burgoon (University of Arizona)
Kathleen M. Carley (Carnegie Mellon University)
Martha Crenshaw (Stanford University)
Adam Dolnik (University Wollongong, Australia)
Martha Feldman (University of California, Irvine)
Robert E. Foster (Office of the Secretary of Defense)
Michael Gabbay (Information Systems Laboratories, Inc)
Marc Genest (Naval War College)
Gregory Godfrey (Metron)
Johanna Gooby (Office of Naval Research)
Robert Higginson (Joint Improvised Explosive Device Defeat Organization)
William Hurley (Institute for Defense Analyses)
Kenneth Israel (Lockheed Martin Company)
Neil F. Johnson (University of Miami)
Edward H. Kaplan (Yale University)
Bryan Kasper (Georgetown University)
Robin Keesee (Joint Improvised Explosive Device Defeat Organization)
Martin Kruger (Office of Naval Research)
Colin Lewis (Consultant)
Edward MacKerrow (Los Alamos National Laboratory)
David Masters (Department of Homeland Security)

Lee Mastroianni (Office of Naval Research)
Clark Richard McCauley (Bryn Mawr College)
Charlene D. Miliken (Department of Homeland Security)
Ray Nelson (Joint Improvised Explosive Device Defeat Organization)
Jimmie C. Oxley (University of Rhode Island)
Michael Pestorius (University of Texas)
Linda Pierce (Army Research Office)
Todd Sandler (University of Texas)
Jacob Shapiro (Princeton University)
Michael Shlesinger (Office of Naval Research)
Allison Smith (Department of Homeland Security)
Mark Stoffel (Office of Naval Research)
Micheline Strand (Army Research Office)
William C. Trogler (University of California, San Diego)
John Waschl (Office of Naval Research)
Ruth P. Willis (Office of Naval Research)
Kevin Wood (Naval Postgraduate School)
Jonathan Young (Pacific Northwest National Laboratory)

NRC Staff

Kathryn Hughes
Kela L. Masters
Jessica L. Pullen
Federico M. San Martini
Ronald D. Taylor

WORKSHOP 2: PREDICTING IED ACTIVITIES (MARCH 17-18, 2008)

Speakers

Jonathan D. Farley (California Institute of Technology)
Alfred O. Hero III (University of Michigan)
Kathleen L. Kiernan (The Kiernan Group)
Daryl Pregibon (Google, Inc.)
Alexander Szalay (Johns Hopkins University)
Pramod K. Varshney (Syracuse University)

Participants

Shabbir Ahmed (Georgia Institute of Technology)
John L. Anderson (Illinois Institute of Technology)
Robert G. Atkins (Massachusetts Institute of Technology, Lincoln Laboratory)
Alan Berman (Consultant)
Nina M. Berry (Joint Improvised Explosive Device Defeat Organization)
Alfred Blumstein (Carnegie Mellon University)
Charles A. Bouman (Purdue University)
Gordon H. Bradley (Naval Postgraduate School)

David J. Brady (Duke University)
Christopher Brown (Office of Naval Research)
Richard Campbell (Bureau of Alcohol, Tobacco, Firearms and Explosives)
Ivy Estabrook (Office of Naval Research)
Anthony Fainberg (Institute for Defense Analyses)
John W. Fisher (Massachusetts Institute of Technology)
Nancy Forbes (Ideal Innovations, Inc.)
Keith Frakes (Army Asymmetric Warfare Office)
William T. Freeman (Massachusetts Institute of Technology)
Mary Lou Fultz (Consultant)
Greg Godfrey (Metron, Inc.)
Maya Gupta (University of Washington)
Robert Higginson (Joint Improvised Explosive Device Defeat Organization)
William J. Hurley (Institute for Defense Analyses)
Kenneth Israel (Lockheed Martin)
Anil K. Jain (Michigan State University)
David Jensen (University of Massachusetts)
Joseph Kielman (Department of Homeland Security)
Gary LaFree (University of Maryland)
Carl Laird (Texas A&M University)
Eva Lee (Georgia Institute of Technology)
Jeffrey Lesho (The Johns Hopkins University, Applied Physics Laboratory)
Colin Lewis (Consultant)
Thomas Lynch (Tier-Tech International, Inc.)
Steven McElroy (Department of Homeland Security)
Charlene Milliken (Department of Homeland Security)
Elan Moritz (US Navy)
Vijay Nair (University of Michigan)
Raymond Nelson (Joint Improvised Explosive Device Defeat Organization)
Jeffrey Norwitz (Naval War College)
Jimmie C. Oxley (University of Rhode Island)
Sonya Proctor (Department of Homeland Security)
Grace Riesling (Bureau of Alcohol, Tobacco, Firearms and Explosives)
Dennis A. Roberson (Illinois Institute of Technology)
Mike Robinson (Army Asymmetric Warfare Office)
Mike F. Shlesinger (Office of Naval Research)
Irma Sityar (Washington Consulting Government Services)
George Solhan (Office of Naval Research)
Marc Steinberg (Office of Naval Research)
Mark Stoffel (Office of Naval Research)
Micheline Strand (Army Research Office)
V.S. Subrahmanian (University of Maryland)
William C. Trogler (University of California, San Diego)
John Waschl (Office of Naval Research)
Larry E. Willis (Department of Homeland Security)
Patrick J. Wolfe (Harvard University)

Jonathan Young (Pacific Northwest National Laboratory)
Randy Zachery (Army Research Office)

NRC Staff

Kathryn Hughes
Kela L. Masters
Jessica L. Pullen
Federico M. San Martini
Ronald D. Taylor
Dorothy Zolandz

GLOSSARY

Agent-based modeling: An adaptive modeling method that simulates the behaviors of individuals to generate data for the analysis of the behaviors of groups

Bayesian networks: A probabilistic graphical model that represents the functional dependencies between a collection of variables of interest

Biometrics: Automated methods of analysis of physical or behavior characteristics for the purpose of identification

Blue forces: A common term referring to "friendly" personnel in an area where conflict is occurring

Data fusion: The formal synthesis of many distinct types of information (audio, visual, written, etc.) to support decision making

Decision theory: A sub-discipline of both game theory and statistics, this is the determination of optimal actions in the presence of uncertainty, when the consequences of those actions are known and depend on various unknown states of nature, which are addressed through the use of probabilistic modeling

Game theory: The study of optimal decision-making in situations that involve a number of players, stipulating either competitive or cooperative interactions between the players, in which their individual payoffs are a function of both their actions and those of the other players, and that involve states of nature which may be only incompletely known

Green forces: A common term referring to the civilians in an area where conflict is occurring

IED: Improvised explosive device

IRA: Provisional Irish Republican Army

JDLR: "Just doesn't look right"

Market-sentiment data: An analysis method used to assess the attitude of a group of consumers

Mixed-initiative decision making: A cyclical method of data training where a user guides a computer program during analysis with the aim of teaching the program how to perform the analysis with greater accuracy

Network tomography: The field of inferential network monitoring, in which internal characteristics of a network are inferred by using information derived from end-point data

Pashtun: The Pashto-speaking people who constitute the majority of the population in Afghanistan

Principal-component analysis: A method used on a set of variables that identifies the primary linear combinations of those variables which account for the majority of the variance in the full set of variables. Its goal is to reduce the dimensionality of a complex data set with many related variables

Probabalistic neural networks: A non-linear statistical model used to fit a response whose structure derives from a model of how information can be combined through the use of a collection of independent sensory nodes

Red forces: A common term referring to the personnel of adversaries in an area where conflict is occurring

Viral marketing: A system of marketing that uses pre-existing social networks to spread a marketing message by encouraging recipients to pass on information

Wiki: A collection of web pages that allows all users to contribute and modify data